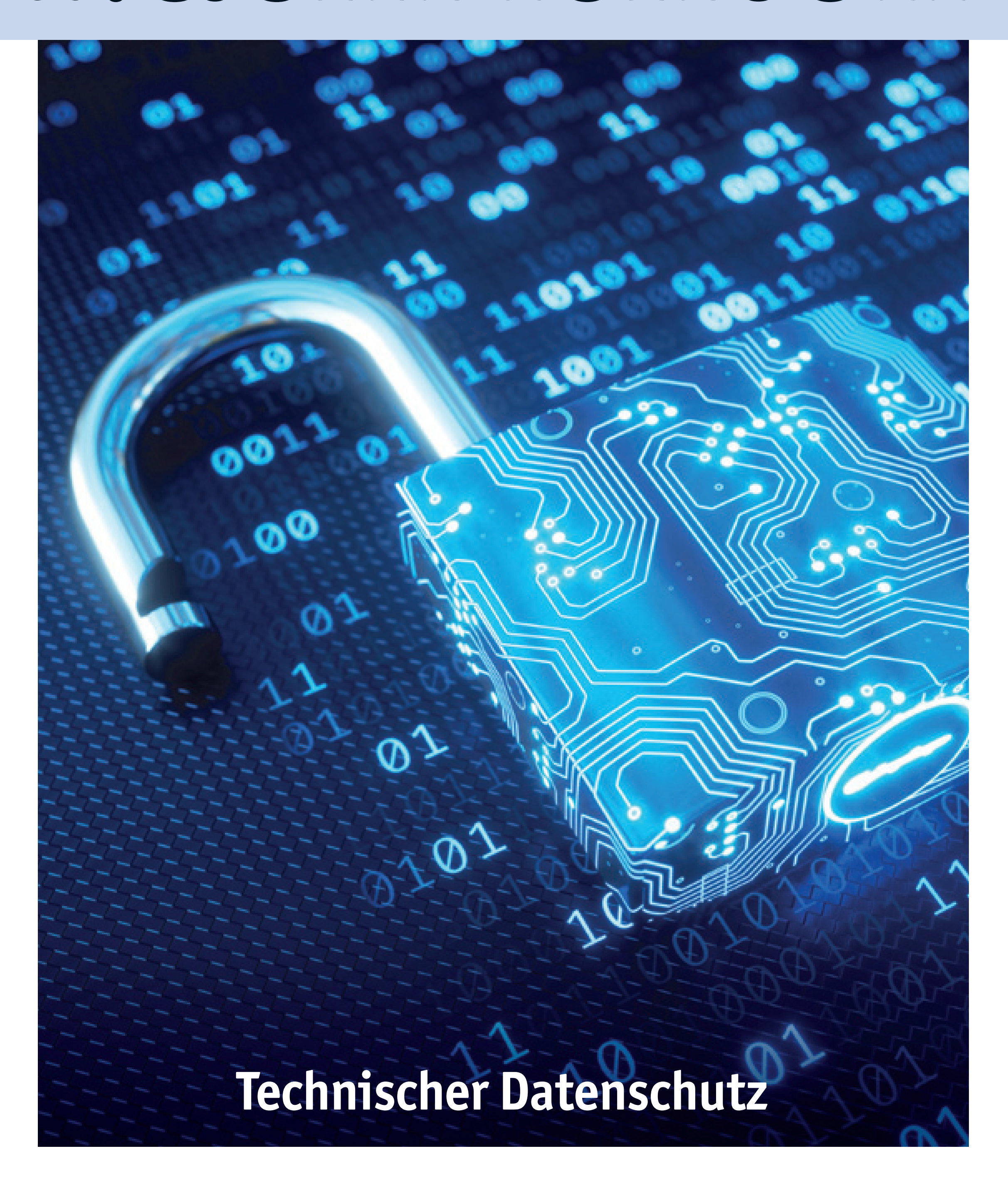
4/2018

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

41. Jahrgang
ISSN 0137-7767
12,00 Euro



Technischer Datenschutz

■ Technischer Datenschutz ■ Die EU-ePrivacy-Verordnung ■ Die Pflicht zur Benennung von Datenschutzbeauftragten bei nichtöffentlichen Stellen ■ Datenschutzfolgenabschätzungen ■ Regulierung des Datenschutzes für Kinder ■ Presserklärungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Montag, 28. Januar 2019
13. Europäischer Datenschutztag
Berlin

Freitag, 01. Februar 2019
Redaktionsschluss DANA 1/2019

Dienstag, 05. Februar 2019
Safer Internet Day 2019 - „Together for a better internet“
weltweit

Samstag, 23. Februar 2019
DVD-Vorstandssitzung
Bonn

MIttwoch, 01. Mai 2019
Redaktionsschluss DANA 2/2019

Samstag, 08. Juni 2019
BigBrotherAwards 2019
Bielefeld

DANA
Datenschutz Nachrichten
ISSN 0137-7767
41. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Werner Hülsmann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, iStock, ClipDealer, Pixabay, AdobeStock,Politiker-Webseiten

Editorial



Ursprünglich war für diese Ausgabe das Schwerpunkthema „Technischer Datenschutz“ geplant. Aber wie das Leben so spielt, werden die Planungen durch das reale Leben über den Haufen geworfen. Zum einen stellte sich die Frage, was gibt es überhaupt Neues zum technischen Datenschutz. Da fand sich dann erstmal nicht ganz so viel, was die Zielgruppe dieser Zeitschrift interessieren dürfte. Zum anderen gab es wichtige (Nicht)-Entwicklungen zum Entwurf der ePrivacy-Verordnung und zu weiteren Omnibusgesetzen, mit denen nationales Recht geändert werden soll. Aus diesen Gründen enthält diese Ausgabe nur einen Artikel, der einige Aspekte des Technischen Datenschutzes beleuchtet.

Dafür finden sich aber – neben den üblichen umfangreichen Datenschutz-Nachrichten aus Bund, Ländern, Europa und der Welt sowie Gerichtsurteilen und Buchbesprechungen – ein Artikel zur Regulierung des Datenschutzes bei Kindern, ein Kommentar zur Datenschutz-Folgenabschätzung (der im weitesten Sinne auch zum ursprünglich vorgesehenen Schwerpunktthema passt) eben auch ein Artikel zum Entwurf der ePrivacy-Verordnung und einer zu den Gesetzesvorhaben auf nationaler Ebene, in denen auch die in Deutschland deutlich umfassender geregelte Pflicht zu Benennung von Datenschutzbeauftragten durch nichtöffentliche Stellen zur Disposition steht.

In der Hoffnung, dass diese Zeitschrift Sie noch rechtzeitig vor dem Jahreswechsel erreicht, wünschen wir Ihnen nicht nur eine spannende Lektüre sondern auch alles Gute im neuen Jahr. Bleiben Sie uns gewogen!

Werner Hülsmann

Stellv. Vorsitzender der Deutschen Vereinigung für Datenschutz

Autorinnen und Autoren dieser Ausgabe:

Kathrin Häring (BSc)
Studentin und Projektbearbeiterin im Master of Media Research an der Hochschule der Medien in Stuttgart, kathrin.haering@gmx.net

Werner Hülsmann
Vorstandsmitglied in der DVD, huelsmann@datenschutzverein.de, Ismaning

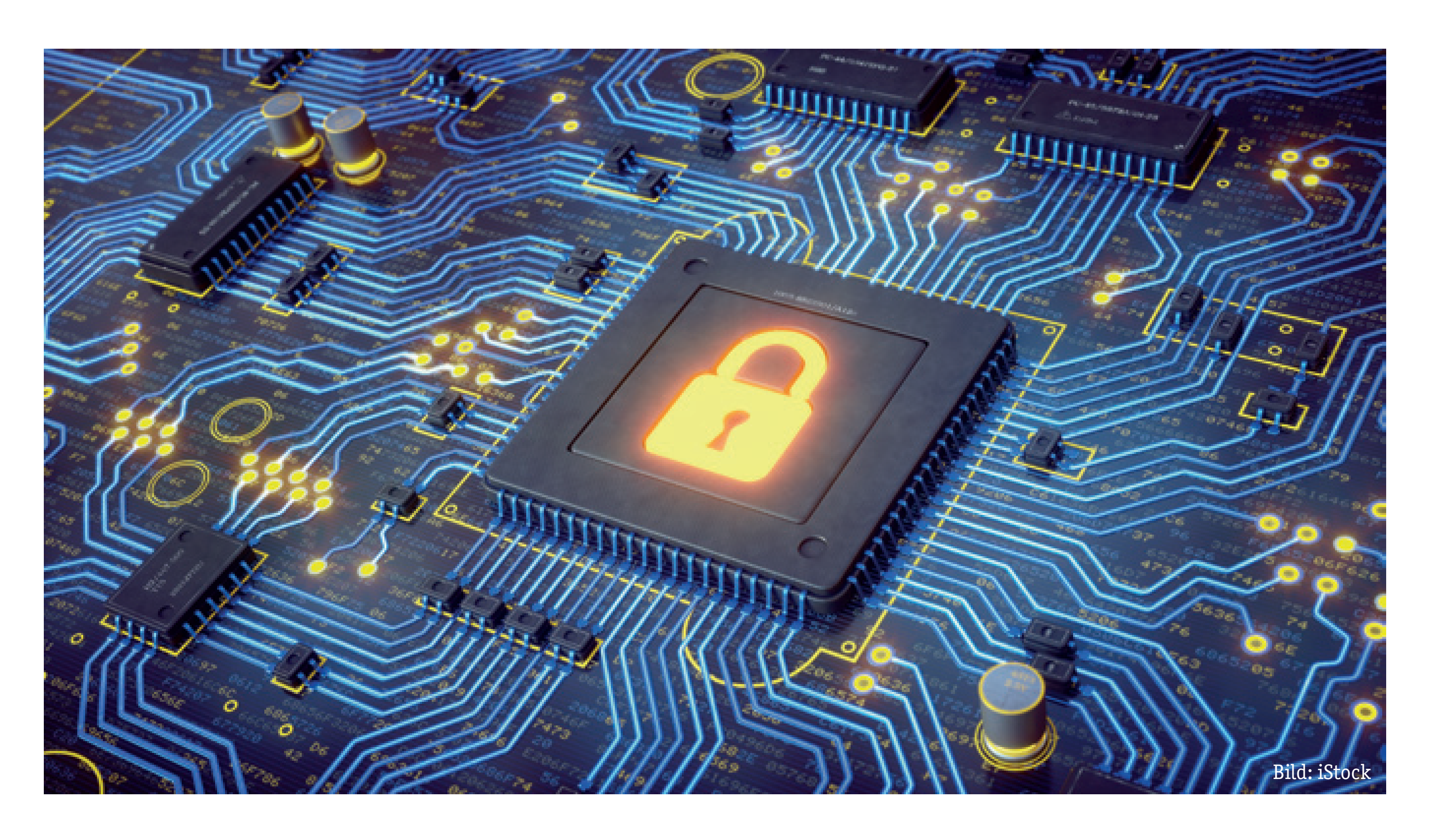
Joachim Jakobs
Freier Journalist und Buchautor, jj@privatsphaere.org

Prof. Holger Nohr
Hochschule der Medien Stuttgart, Master of Media Research, nohr@hdm-stuttgart.de

Werner Hülsmann

Technischer Datenschutz – was gibt es Neues?

Dokumentation der technischen und organisatorischen Maßnahmen


Bild: iStock

Auftragnehmer, wie die Auftragsverarbeiter in Zeiten vor der Gültigkeit der DSGVO hießen, kannten diese Dokumentationspflicht bereits, da die Dokumentation der TOM Bestandteil der Vereinbarung oder des Vertrags zur Auftragsdatenverarbeitung (ADV-Vereinbarung) gemäß § 11 des alten Bundesdatenschutzgesetzes (BDSG-alt) war. Nach herrschender Meinung ist auch mit Gültigwerden der DSGVO weiterhin für Vereinbarungen oder Verträge zur Auftragsverarbeitung (AVV) verpflichtend die TOM schriftlich oder zumindest in Textform zu dokumentieren, denn nur so könne der Verantwortliche sicherstellen, dass er, wie es Art. 28 Abs. 1 DSGVO verlangt, „nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet", zusammenarbeitet. Ohne eine Dokumentation der TOM des Auftragsverarbeiters lässt es sich nicht überprüfen, ob der Auftragsverarbeiter diese „hinreichenden Garantien" gewährleistet.

Inzwischen sollte es sich aber auch herumgesprochen haben, dass jeder Verantwortliche (Unternehmen, Behörden und andere Stellen im Sinne des Art. 4 Ziff. 7 DSGVO) die technischen und organisatorischen Maßnahmen (TOM), die dazu dienen, die Sicherheit der Datenverarbeitung zu gewährleisten[1], dokumentieren muss. Dies ergibt sich bereits aus den Regelungen zum Verzeichnis der Verarbeitungstätigkeiten (hier: Art. 30 Abs. 1 Buchst. g DSGVO für Verantwortliche und Art. 30 Abs. 2 Buchst. d DSGVO für Auftragsverarbeiter[2]). Auch zur Umsetzung der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO ist die Dokumentation der TOM erforderlich.

Die DSGVO gibt nun aber keine konkreten Vorgaben, wie und in welcher Ausführlichkeit die TOM zu dokumentieren sind. Mit etwas Suchen finden sich bei der Dt. Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder) in dem Anwendungshinweis „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO" (Stand: Februar 2018)[3] nützliche Empfehlungen zur Dokumentation der TOM:

„Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell, die Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen." (Ziffer 6.7)

Unter Ziffer 6.8 werden „Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben“ ausführlich erläutert und unter Ziffer 6.9 werden „weitere Maßnahmenbereiche, die sich aus der DS-GVO ergeben und deren Darstellung im Verzeichnis empfohlen wird“ umfassend dargestellt. Wer also als Verantwortlicher oder Auftragsverarbeiter seine TOM dokumentieren will, dem ist die Lektüre zumindest der Ziffern 6.7 bis 6.9 dieser Hinweise sehr zu empfehlen.

Standard-Datenschutzmodell (SDM)

Das Standard-Datenschutzmodell wurde im April 2018 in der Version 1.1 von der Dt. Datenschutzkonferenz veröffentlicht[4]. Es ist laut seiner Beschreibung „eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“. In der Einleitung finden sich folgende Aussagen

„Das Standard-Datenschutzmodell (SDM) bietet geeignete Mechanismen, um diese rechtlichen Anforderungen der DS-GVO in technische und organisatorische Maßnahmen zu überführen. Zu diesem Zweck strukturiert das SDM die rechtlichen Anforderungen in Form der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit. Das SDM überführt mit Hilfe dieser Gewährleistungsziele die rechtlichen Anforderungen der DS-GVO in die von der Verordnung geforderten technischen und organisatorischen Maßnahmen. Das SDM enthält im Anhang einen Referenzkatalog von technischen und organisatorischen Maßnahmen. Dieser Katalog kann herangezogen werden, um bei jeder einzelnen Verarbeitung sowohl durch den Verantwortlichen selbst als auch durch die Aufsichtsbehörde zu prüfen, ob das rechtlich geforderte Soll von Maßnahmen mit dem vor Ort vorhandenen Ist von Maßnahmen übereinstimmt. Das SDM und der Maßnahmenkatalog bieten zudem eine sehr gut geeignete Grundlage für die Planung und Durchführung der von der DS-GVO geförderten datenschutzspezifischen Zertifizierungen (Art. 42 DS-GVO) und der in bestimmten Fällen erforderlichen Datenschutz-Folgenabschätzung (Art. 35 DS-GVO).“ (SDM, Version 1.1 S. 5f)

Mit dieser Beschreibung könnte das SDM „das“ Tool zur Dokumentation der TOM sein. Wenn, ja wenn nicht das Kapitel „12 Maßnahmenkatalog“ nur einen Hinweis enthielte, dass der Maßnahmenkatalog „künftig Bestandteil des SDM“ sein wird.

Aber es gibt Hoffnung. Am 7. September 2018 wurden von der Unterarbeitsgruppe „SDM-Bausteine“ (zu dieser gehören: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Sächsischer Datenschutzbeauftragter, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland) die ersten sieben Maßnahmenbausteine veröffentlicht[5]. Die Themen dieser Bausteine sind:

- 11 Aufbewahrung
- 41 Planung / Spezifikation
- 42 Dokumentation
- 43 Protokollierung
- 50 Trennung
- 60 Löschen
- 80 Datenschutz-Management

Diese Nummerierung macht neugierig auf die offensichtlich schon entwickelte Struktur dieser Bausteine. Wichtig bei der Nutzung der Bausteine ist der Hinweis:

„Die Autoren der Unterarbeitsgruppe weisen ausdrücklich darauf hin, dass diese Bausteine noch nicht in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder abgestimmt worden sind. Sie empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der Bausteine den an der Entwicklung der Bausteine beteiligten Datenschutzbehörden mitzuteilen (z. B. unter sdm@datenschutz-mv.de), und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.“

Zu finden sind diese Maßnahmenbausteine auf https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ unter „Maßnahmenkatalog“ als PDF-Dateien. In den einzelnen Bausteinen ist neben einer Darstellung der Vorgaben auch eine Liste möglicher Maßnahmen aufgeführt. Auch wenn es sich bisher erst um sieben Maßnahmenbausteine handelt, lohnt sich ein Blick in diese. Wenn die noch fehlenden Maßnahmenbausteine zeitnah erstellt werden – auch mit Hilfe der Anwenderinnen und Anwender – kann das SDM zu einem gut nutzbaren Tool zur Dokumentation der TOM und weit darüber hinaus werden.

Geldbußen wegen nicht ausreichender TOM

Gleich zwei Vorfälle, bei denen Aufsichtsbehörden Geldbußen wegen nicht ausreichender TOM erlassen haben, sind in der letzten Zeit publik geworden.

400.000 € Geldbuße für ein Krankenhaus in Portugal

Ein Krankenhaus in Portugal wurde von der dortigen Datenschutz-Aufsichtsbehörde wegen DSGVO-Verstößen mit einer Geldbuße von 400.000 € belegt. Das Krankenhaus will allerdings gegen diese Geldbuße klagen. Ob die Klage Aussicht auf Erfolg hat, würde der Autor auf Basis des Zeitungsartikels[6] allerdings bezweifeln: „Laut dem Zeitungsbericht hat der Krankenhausbetreiber Untersuchungen der Datenschützer zufolge „bewusst“ IT-Technikern Zugang zu Daten verschafft, die eigentlich nur von Ärzten hätten eingesehen werden dürfen. Durch einen Test sei festgestellt worden, dass solch ein Profil mit unbegrenztem Zugang problemlos erstellt werden konnte. - Und nicht nur das: Obwohl 2018 nur 296 Ärzte in dem Krankenhaus arbeiten, waren in dem System insgesamt 985 aktive Benutzer als „Arzt“ registriert.“ Alleine diese wenigen Aussagen machen deutlich, dass hier die Vertraulichkeit der Daten (eine der Forderungen aus Art. 5 und aus Art. 32 DSGVO) nicht gewährleistet ist und entsprechende TOM nicht in ausreichender Form umgesetzt wurden.

20.000 € Geldbuße für einen baden-württembergischen Social-Media-Anbieter

Mit dieser Geldbuße wurde die erste Geldbuße auf Grundlage der DSGVO in Deutschland verhängt. Laut der Pressemitteilung der baden-württembergischen Datenschutzaufsichtsbehörde[7]

vom 22. November 2018 ist das Bußgeld so glimpflich ausgefallen, da das Unternehmen mit der Aufsichtsbehörde, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI), kooperiert habe:

„Das Unternehmen hatte sich am 08. September 2018 mit einer Datenpannenmeldung an den LfDI gewandt, nachdem es bemerkt hatte, dass durch einen Hackerangriff im Juli 2018 personenbezogene Daten von circa 330.000 Nutzern, darunter Passwörter und E-Mail-Adressen, entwendet und Anfang September 2018 veröffentlicht worden waren. Ihre Nutzer informierte das Unternehmen nach den Vorgaben der EU-Datenschutzgrundverordnung (DS-GVO) unverzüglich und umfassend über den Hackerangriff. Gegenüber dem LfDI legte das Unternehmen in vorbildlicher Weise sowohl Datenverarbeitungs- und Unternehmensstrukturen als auch eigene Versäumnisse offen. Hierdurch wurde dem LfDI bekannt, dass das Unternehmen die Passwörter ihrer Nutzer im Klartext, mithin unverschlüsselt und unverfremdet (ungehasht), gespeichert hatte. (...).

Das Unternehmen setzte innerhalb weniger Wochen weitreichende Maßnahmen zur Verbesserung ihrer IT-Sicherheitsarchitektur um und brachte damit die Sicherung ihrer Nutzerdaten auf den aktuellen Stand der Technik. Zudem wird das Unternehmen innerhalb der nächsten Wochen in Abstimmung mit dem LfDI zusätzliche Maßnahmen zur weiteren Verbesserung der Datensicherheit durchführen.

Durch die Speicherung der Passwörter im Klartext verstieß das Unternehmen wissentlich gegen seine Pflicht zur Gewährleistung der Datensicherheit bei der Verarbeitung personenbezogener Daten gem. Art. 32 Abs. 1 lit a DS-GVO."

Die moderate Höhe des Bußgeldes wurde vom LfDI damit begründet, dass Bußgelder nach der DSGVO nicht nur wirksam und abschreckend, sondern auch verhältnismäßig sein sollen. Zusammen mit dem Bußgeld habe das Unternehmen unter Einbeziehung der seit der Datenschutzpanne ergriffenen Maßnahmen und künftig noch vorgesehen IT-Sicherheitsmaßnahen einen Gesamtbetrag im sechsstelligen Euro-Bereich zu tragen. Da andere Medien auch den Namen des Unternehmens genannt haben, könnte es gut sein, dass es neben dieser Geldbuße zusätzlich auch zu Reputationsverlusten und Abwanderung von Kundinnen und Kunden und damit zu monetären Einbußen kommt.

Fazit

Auch wenn die Umsetzung sowie die Dokumentation der TOM mit Aufwand verbunden ist, so lohnt es sich doch, hier für ausreichende Maßnahmen zu sorgen und diese auch zu dokumentieren. Dies dient nicht nur dem Schutz der Privatsphäre der betroffenen Personen, sondern reduziert auch das Risiko von Bußgeldern.

1 Vgl. Art. 24 Abs. 1 und Art. 32 Abs. 1 in Verbindung mit Art. 5 DSGVO

2 Dort steht zwar jeweils „wenn möglich" – Es ist aber nicht ersichtlich, warum dies spätestens zum Zeitpunkt des Ein- möglich sein sollte.

3 https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf

4 https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_sdm.pdf

5 https://www.datenschutz-mv.de/datenschutz/publikationen/Erste-Bausteine-des-SDM-Maßnahmenkatalogs/

6 http://www.faz.net/aktuell/wirtschaft/diginomics/dsgvo-strafe-krankenhaus-in-portugal-muss-400-000-euro-zahlen-15852321.html

7 https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/

Werner Hülsmann

Die EU-ePrivacy-Verordnung – eine unendliche Geschichte?

Eigentlich sollte die EU-ePrivacy-Verordnung (ePrivVO) bereits am 25. Mai 2018 gemeinsam mit der EU-Datenschutzgrundverordnung (DSGVO) gültig werden. Tatsächlich ist sie immer noch nicht gültig. Derzeit ist leider auch nicht davon auszugehen, dass die ePrivVO vor 2021 gültig werden wird. Zwar war das EU-Parlament in Sachen ePrivVO schon sehr fleißig. Aber der Ministerrat lässt sich Zeit, viel Zeit, sehr viel Zeit, um nicht zu sagen unverschämt viel Zeit. Aber der Reihe nach:

Immer noch gültig: Die ePrivacy-Richtlinie

Derzeit ist auf EU-Ebene die sogenannte ePrivacy-Richtlinie („RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)" oder kürzer: ePrivRL) in der aktuellen Fassung gültig. Die letzte wesentliche Änderung erfolgte durch die sogenannte Cookie-Richtlinie (RICHTLINIE 2009/136/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2009).

Die ePrivacy-Richtlinie ist mitsamt ihren Änderungen allerdings – wie dies bei EU-Richtlinien grundsätzlich so ist – nicht direkt anwendbar, sondern musste, damit sie in den Mitgliedstaaten der EU wirksam wurde, von diesen in nationales Recht umgesetzt werden. Diese Umsetzung ist in den verschiedenen Mitgliedstaaten sehr unterschiedlich erfolgt. Dies wird beispielsweise bei der Umsetzung



Bild: iStock

des Art. 13 dieser Richtlinie deutlich. So sind in Deutschland die Regelungen zur werblichen Ansprache per Telefon, Fax, E-Mail, etc. aus Art. 13 ePrivRL im § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) gelandet. Dies hat zur Konsequenz, dass eine unzulässige werbliche Ansprache per E-Mail nur einen Wettbewerbsverstoß darstellt, die Datenschutzaufsichtsbehörden sich hier nicht zuständig fühlen und der Verstoß nicht mit einem Bußgeld geahndet wird. Andere Regelungen der ePrivRL sind in Deutschland durch Regelungen im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG) umgesetzt worden.

In Spanien war und ist eine unzulässige werbliche Ansprache per E-Mail allerdings sehr wohl ein Verstoß, der mit einem Bußgeld geahndet wurde und wird. So hat es in den letzten Jahren einige Fälle gegeben, in denen Bußgelder in fünfstelliger Höhe verhängt wurden.

Die Umsetzung der Änderungen an der ePrivacy-Richtlinie, die sich aus der Cookie-Richtlinie ergaben, hätten bis 2011 auch in Deutschland erfolgen müssen. Zwar behauptete die Bundesregierung beharrlich gegenüber der EU-Kommission, dass diese Umsetzung erfolgt sei. Faktisch betrachtet kann in Deutschland aber keine Rede davon sein, dass es eine adäquate Umsetzung der wesentlichen Vorschrift der Cookie-Richtlinie gegeben hätte, nach der für alle Cookies, die nicht technisch notwendig sind und deren Gültigkeitsdauer über das Sitzungsende hinausgeht, eine Einwilligung der jeweiligen Nutzerinnen und Nutzer erforderlich ist.

Was änderte sich durch das Gültigwerden der DSGVO

Kurz gesagt: Fast nichts. Artikel 95 DSGVO, der schon ausweislich seiner Überschrift das „Verhältnis zur Richtlinie 2002/58/EG“ also der ePrivacy-Richtlinie regelt, bestimmt, dass die DSGVO „natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf[erlegt], soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.“ Die ePrivacy-Richtlinie bleibt also im Wesentlichen durch die DSGVO unberührt.

Zu berücksichtigen ist aber, dass gemäß Artikel 2 Satz 1 ePrivRL die Begriffsbestimmungen der zum 25. Mai 2018 aufgehobenen EU-Datenschutzrichtlinie (Richtlinie 95/46/ EG) gelten und dass nach Artikel 2 Satz 2 Buchst. f der Begriff „‘Einwilligung‘ eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/ EG;“ bezeichnet. Diese Verweise auf die alte EU-Datenschutzrichtlinie laufen aber nun nicht ins Leere, sondern sind gemäß Art. 94 Abs. 2 DSGVO als solche auf die DSGVO zu sehen. Sprich: Für Einwilligungen gemäß der – durch die Cookie-Richtlinie geänderten – ePrivacy-Richtlinie sind die Anforderungen an die Einwilligung aus den Art. 7 und 8 DSGVO zu stellen. Letzteres ist nicht nur beim Setzen von Cookies, deren Gültigkeitsdauer über die aktuelle Browsersitzung hinausgeht zu beachten, sondern auch bei der werblichen Ansprache per elek-

tronischer Medien, wie Telefon, Fax, E-Mail, etc. für die auch nach dem Gültigwerden der DSGVO die Regelungen des § 7 UWG als deutsche Umsetzung von Art. 13 ePrivRL weiterhin zu beachten sind.

Der Entwurf der ePrivacy-Verordnung

Schon bei der Vorstellung des Entwurfs der DSGVO war seitens der EU-Kommission angekündigt worden, dass auch eine Überarbeitung der EU-ePrivacy-Richtlinie vorgesehen ist. Eine entsprechende öffentliche Konsultation hierzu hat bereits im Zeitraum vom 12. April bis 05. Juli 2016 stattgefunden. Die Zusammenfassung des Ergebnisses dieser Konsultation wurde von der EU-Kommission am 04. August 2016 veröffentlicht[1].

Die EU-Kommission hat sich, auch auf Grund der Ergebnisse der Konsultation, entschieden, wie schon bei der DSGVO auch für den Bereich der elektronischen Kommunikation einen Entwurf für eine direkt gültige Verordnung vorzulegen und es nicht bei einer Richtlinie zu belassen[2]. Bereits am 13. Dezember 2016 wurde ein erster Entwurf geleakt[3]. Am 10. Januar 2017 wurde von der EU-Kommission der – gegenüber dem geleakten vorläufigen Entwurf noch veränderte – Entwurf der „VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)“ oder kurz: ePrivacy-Verordnung[4] vorgestellt. In diesem Entwurf war noch vorgesehen, dass die ePrivacy-Verordnung zeitgleich mit der DSGVO am 25. Mai 2018 gültig werden sollte. Der EU-Kommission war selbstverständlich klar, dass dies ein ambitionierter Zeitplan war. Er wäre – bei gutem Willen aller Beteiligten – aber einzuhalten gewesen. Aber offensichtlich war und ist – wie noch gezeigt wird – nicht überall dieser gute Wille vorhanden.

Das EU-Parlament war fleißig

Bereits am 16. Februar 2017 erfolgte die Behandlung des Entwurfs der ePrivacy-Verordnung in erster Lesung im Parlament. Es erfolgte eine Verweisung an die Ausschüsse, als federführender Ausschuss wurde – wie es auch bei der Behandlung der DSGVO war – der LIBE-Ausschuss (Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres) bestimmt.

Wie zu erwarten war, wurden sehr viele Änderungsvorschläge eingereicht. Trotzdem gab es schon am 09. Juni 2017 einen ersten Berichtsentwurf der Berichterstatterin des LIBE-Ausschusses[5]. Etwas mehr als vier Monate später, am 19. Oktober 2017, wurde im LIBE-Ausschuss der finale Berichtsentwurf mit 31:24:1 Stimmen angenommen. In gleicher Sitzung hat sich der LIBE-Ausschuss das Mandat zur Aufnahme der Trilog-Verhandlungen erteilt. Dieses LIBE-Trilog-Mandat wurde – entsprechend der geltenden Verfahrensregelungen – am 23. Oktober 2017 im EU-Parlament angekündigt. Da von einigen Fraktionen eine Abstimmung im Parlament verlangt wurde, erfolgte diese am 26. Oktober 2017. Dabei hat das EU-Parlament mit einer deutlichen Mehrheit von 320 zu 280 Stimmen bei 18 Enthaltungen das LIBE-Trilog-Mandat und damit auch den Änderungsvorschlag des LIBE-Ausschusses bestätigt.[6] Da im Änderungsentwurf des LIBE-Ausschusses bereits eine einjährige Übergangszeit vorgesehen war, war zu diesem Zeitpunkt schon ziemlich sicher, dass die ePrivacy-Verordnung nicht vor Ende 2018 gültig werden würde.

Der EU Ministerrat lässt sich Zeit

Eine erste Behandlung des Entwurfs der ePrivacy-Verordnung im Ministerrat erfolgte dagegen erst am 09. Juni 2018. Am 08. September 2017 gab es einen ersten Entwurf der Änderungsvorschläge des Ministerrates[7]. Allerdings gab es erst am 06. Oktober 2017 eine abgestimmte Fassung der Änderungsvorschläge zu den Artikeln 1 bis 5 ePrivVO-Entwurf und der entsprechenden Erwägungsgründe[8]. Zehn Tage später, am 16. Oktober 2017 wurde die abgestimmte Fassung der Änderungsvorschläge zu den Artikeln 12 bis 20 ePrivVO-Entwurf und den entsprechenden Erwägungsgründen veröffentlicht[9]. Es fehlten also im November 2017 immer noch die abgestimmten Änderungsvorschläge zu den Artikeln 6 bis 11 und den Artikeln 21 bis 29 ePrivVO-Entwurf. Auch der Ministerrat hatte eine einjährige Übergangsfrist vorgesehen, so dass von dieser Seite aus ein Gültigwerden vor Ende 2018 nun bereits ausgeschlossen werden konnte.

Ein Jahr später, im November 2018, ist der ePrivVO-Entwurf immer noch in der Beratung des EU-Ministerrats. Der Ministerrat hat seine Stellungnahme noch immer nicht beschlossen. Daran hat auch die österreichische Ratspräsidentschaft (01.07. bis 31.12.2018) nichts geändert. Zwar steht im „Programm des österreichischen Ratsvorsitzes“:

„Überdies wird sich der österreichische Ratsvorsitz für zukunftssichere Regelungen zum Datenschutz im digitalen Umfeld einsetzen, insbesondere im Rahmen der Arbeiten zur Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation. Dabei gilt es einerseits einen hohen Schutz der Privatsphäre in der elektronischen Kommunikation sicherzustellen und andererseits Rücksicht auf die Entwicklungsmöglichkeiten für innovative Dienste zu nehmen.“[10]

Von entsprechenden Aktivitäten, die zu einem Abschluss der Beratungen des Entwurfs der ePrivacy-Verordnung führen könnten, ist allerdings nichts zu sehen. Ganz im Gegenteil: Die österreichische Ratspräsidentschaft hat das Verfahren im Rat mehr oder weniger neu aufgerollt. Am 19. Oktober 2018 hat die österreichische Ratspräsidentschaft einen neuen Entwurf einer Stellungnahme des Rats veröffentlicht[11]. Dieser müsste nun im Ministerrat erörtert werden, wenn er die Basis für den Beschluss der Stellungnahme werden soll. Von daher ist deutlich, dass Österreich kein Interesse daran hat, die Verhandlungen im Rat bis zum Ende der österreichischen Ratspräsidentschaft abzuschließen. Während der sechsmonatigen österreichischen Ratspräsidentschaft ist auch nur eine Sitzung des Ministerrats für „Transport, Telekommunikation und Energie“ angesetzt. Diese findet nach Redaktionsschluss am 03. und 04. Dezember 2018 statt und hat immerhin einen „Fortschrittsreport“ zur ePrivacy-Verordnung auf der Tagesordnung[12]. Offensichtlich scheint die österreichische Ratspräsidentschaft lieber EU-Überwachungsrichtlinien zu forcieren

als die ePrivacy-Verordnung voranzubringen[13].

Auch Deutschland und Frankreich „glänzen" als Bremser bei der ePrivacy-Verordnung, u.a. aufgrund von massiver Lobbyarbeit der Werbewirtschaft und Firmen, die ihr Geld mit den Daten der Nutzerinnen und Nutzer verdienen.

Die nächsten Schritte?

Erst wenn der Ministerrat seine Stellungnahme beschlossen hat, können die Trilog-Verhandlungen (zwischen EU-Kommission, EU-Parlament und EU-Ministerrat) beginnen. In diesen wird dann der endgültige Text der ePrivacy-Verordnung festgelegt. Aber selbst wenn die Trilog-Verhandlungen noch 2019 abgeschlossen werden sollten, kann die ePrivacy-Verordnung frühestens 2020 oder sogar erst 2021 – der österreichische Entwurf der Stellungnahme des Ministerrats sieht eine zweijährige Übergangsfrist vor – gültig werden. Bis dahin müssen leider Nutzerinnen und Nutzer wie auch Firmen und andere Stellen mit einem nicht immer einfachen Dreiklang aus DSGVO, ePrivacy-Richtlinie und den mehr oder weniger guten Umsetzungen der ePrivacy-Richtlinie in nationales Recht leben.

NGOs fordern EU-Rat zum Beschluss über qualifizierte ePrivacy-Verordnung auf

In einem offenen Brief [14] vom 27. Oktober 2018 fordern alleine in Deutschland 16 Nichtregierungsorganisationen (NGO) den Bundesminister für Wirtschaft und Energie auf, sich für einen Abschluss der Verhandlungen zur ePrivacy-Verordnung einzusetzen, da dies „ein großer Schritt zur Stärkung des Rechts des Einzelnen auf Privatsphäre und Meinungsfreiheit in der gesamten EU, zur Stärkung des Vertrauens in Online-Dienste und zur Schaffung von Rechtssicherheit für Unternehmen und Einzelpersonen wäre". Die Deutsche Vereinigung für Datenschutz hat diesen Brief ebenfalls unterzeichnet und hierzu am 30. Oktober 2018 eine eigene Pressemitteilung veröffentlicht, die auch in dieser Ausgabe abgedruckt ist. Auch in anderen Ländern der EU wurden vergleichbare offene Briefe an die jeweiligen zuständigen Ministerien gesandt.

Worum geht es?

Ein wesentlicher Streitpunkt bei der ePrivacy-Verordnung ist die Frage, ob eine Nutzung von Standort- und weiteren Telekommunikationsverkehrsdaten für „kompatible Zwecke" durch die ePrivacy-Verordnung zugelassen werden soll. Diese Fragestellung ist für das Fernmeldegeheimnis und den Schutz der Privatsphäre grundlegend! Derzeit gilt aus guten Gründen, dass Standortdaten nur genutzt werden dürfen, soweit dies für die Erbringung des Dienstes erforderlich ist oder wenn eine Einwilligung der betroffenen Person vorliegt. Lobbygruppen der Wirtschaft fordern dagegen, es zu erlauben auf Basis der aus dem allgemeinen Datenschutzrecht bekannten Interessenabwägung (Art. 6 Abs. 1 Buchst. f DSGVO) diese – und andere Verkehrsdaten – auch für sogenannte kompatible Zwecke zu nutzen. Dabei wird von diesen Lobbygruppen aber – vermutlich bewusst – übersehen, dass es sich bei diesen Verkehrs- und Standortdaten bereits um sehr sensible Daten handelt, deren Verwendung durch Unternehmen und staatliche Stellen zur Wahrung der Persönlichkeitsrechte der betroffenen Personen strengeren Regelungen unterworfen werden müssen, als sie im allgemeinen Datenschutzrecht enthalten sind. Auch die DSGVO kennt mit den Artikeln 9 und 10 strikte Einschränkungen für besonders sensible Datenkategorien, bei denen eine Verarbeitung auf Basis der Interessenabwägung aus gutem Grund ausgeschlossen ist. Gleiches muss auch weiterhin für die Verkehrs- und Standortdaten im Bereich der Telekommunikation gelten[15], da diese bereits tiefgehende Einblicke in Verhalten und Vorlieben der betroffenen Personen gewähren.

Ausblick

Aus EU-Parlamentskreisen ist zu hören, es würde sich nicht lohnen, den österreichischen Entwurf der Stellungnahme anzuschauen, da auch dieser erst im Rat diskutiert werden müsse. Es sei auch derzeit nicht absehbar, wann und unter welcher Ratspräsidentschaft der Entwurf der ePrivacy-Verordnung erörtert und die dazugehörige Stellungnahme beschlossen würde. Österreich sitzt dem Rat nur noch bis Ende Dezember 2018 vor, dann folgen Rumänien (Januar - Juni 2019), Finnland (Juli - Dezember 2019), Kroatien (Januar - Juni 2020) und Deutschland (Juli - Dezember 2020)[16]. Ob eines dieser Länder die Behandlung des Entwurfs der ePrivacy-Verordnung vorantreiben wird, bleibt abzuwarten.

Im EU-Parlament und insbesondere im LIBE-Ausschuss wird derzeit überlegt, ob das EU-Parlament vor der im Mai 2019 anstehenden nächsten Wahl des EU-Parlamentes abschließend über den Entwurf der ePrivacy-Verordnung entscheiden soll. Üblicherweise findet diese abschließende Entscheidung nach den Trilog-Verhandlungen auf Basis des in den Trilog-Verhandlungen ausgehandelten Textes statt. Eine vorherige abschließende Entscheidung des EU-Parlaments zum Entwurf der ePrivacy-Verordnung hätte allerdings eine gewisse bindende Wirkung auf das Verhandlungsmandat des LIBE-Ausschusses der nächsten Legislaturperiode.

Ein Ende der „unendlichen Geschichte ePrivacy-Verordnung" ist also leider noch nicht in Sicht. Auch ist nicht abzusehen, ob diese „Geschichte" ein gutes Ende nehmen wird. Der Autor dieser Zeilen hofft, dass es nicht weitere zwei Jahre dauert bis es sich lohnt, hier in der DANA erneut über die ePrivacy-Verordnung zu berichten.

1 Siehe: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive

2 Vgl. http://europa.eu/rapid/press-release_IP-17-16_de.htm

3 Siehe: https://dsgvo.expert/oh6Xp und Hülsmann: „Entwurf der ePrivacy-Verordnung ist öffentlich – Auswirkung auf das Direktmarketing?", DANA 4/2016 Seite 177ff

4 Die am 14. Februar 2017 veröffentlichte deutsche Übersetzung des Entwurfs ist hier zu finden: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42678

5 https://dvd-ev.de/20170003

6 Vgl. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0324&language=EN

7 Vgl. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT&qid=1505069080801&from=EN

8 http://data.consilium.europa.eu/doc/document/ST-12955-2017-INIT/EN/pdf

9 Vgl. http://data.consilium.europa.eu/doc/document/ST-13217-2017-INIT/en/pdf

10 https://www.eu2018.at/dam/jcr:b5dd3521-d93b-4dbc-8378-1d1a6a7f99cf/Programm%20des%20%C3%B6sterreichischen%20Ratsvorsitzes.pdf

11 Vgl. https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf

12 https://www.consilium.europa.eu/media/36332/st_10497_2018_init_en.pdf

13 Vgl. https://www.eu2018.at/de/agenda-priorities/priorities.html

14 https://dvd-ev.de/Brief-ePriv

15 Vgl. auch https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_de

16 https://www.consilium.europa.eu/de/council-eu/presidency-council-eu/

Werner Hülsmann

2. DSAnpUG-EU, DSUAnpaG-EU und die Pflicht zur Benennung von Datenschutzbeauftragten bei nichtöffentlichen Stellen

Ja, Sie haben richtig gelesen. Es gibt aktuell nicht nur einen Gesetzesentwurf zur Anpassung und Umsetzung von Bundesrecht an die DSGVO und die JI-Richtlinie, sondern es gibt

- zum einen den Entwurf des 2. DSAnpUG-EU (Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU) - BT-Drs. 19/4674)[1], der zumindest in Datenschutzkreisen schon bekannt war und
- zum anderen den Entwurf eines „Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679" - BT-Drs. 19/4671[2], von dem auch der Autor dieses Beitrags bis Mitte Oktober noch nichts gehört und gelesen hatte.

Für den zweiten Gesetzentwurf gibt es keine offizielle Abkürzung, auch wenn sich Datenschutzumsetzungs- und Anpassungsgesetzentwurf EU (noch kürzer: DSUAnpG-EU) anbieten würde. Während das 2. DSAnpUG-EU wie das erste DSAnpUG-EU aus dem Bundesinnenministerium kommt und in erster Linie der Anpassung nationalen Rechts an die DSGVO und in zweiter Linie der Umsetzung der Richtlinie (EU) 2016/680 (JI-Richtlinie) dient, dient das Datenschutzumsetzungs- und Anpassungsgesetz EU in erster Linie der Umsetzung der JI-Richtlinie und in zweiter Linie der Anpassung nationalen Rechts an die DSGVO. Das kommt Ihnen etwas verwirrend vor. Keine Sorge, das ist es auch. Ob das Absicht ist? Diese Frage möge die geneigte Leserin und der geneigte Leser bitte für sich selbst – nach der Lektüre dieses Beitrags – beantworten. Mit diesen beiden Gesetzentwürfen sollen insgesamt 173 Bundesgesetze geändert werden. Das sind nicht gerade wenige. Alle diese Änderungen nachzuvollziehen bedeutet einen immensen Arbeitsaufwand.

Das 2. DSAnpUG-EU ist im Rahmen der Verbändeanhörung auch der Deutschen Vereinigung für Datenschutz mit der Bitte um Stellungnahme zugeleitet worden. Diese Fassung diente tatsächlich in erster Linie redaktioneller Anpassungen an die DSGVO und einiger Umsetzungen der JI-Richtlinie. Die dann später in den Bundesrat und den Bundestag eingebrachte Fassung sah da schon ganz anders aus und enthält auch Regelungen zur deutlichen Einschränkung des Datenschutzes (siehe „Auszüge aus dem Plenarprotokoll vom 12. Oktober 2018").

Im Rahmen der Gesetzgebungsverfahren zu den beiden Gesetzentwürfen ist im Oktober erst einmal die Initiative aus Bayern im Bundesrat, mit der die deutschen Regelungen zur Pflicht zur Benennung betrieblicher Datenschutzbeauftragter des § 38 Abs. 1 BDSG gestrichen bzw. deutlich aufgeweicht werden sollten, gescheitert (nur Baden-Württemberg hat noch für diese Initiative gestimmt). Das Thema der Einschränkung der Benennungspflicht von Datenschutzbeauftragten für nichtöffentliche Stellen ist damit aber noch nicht vom Tisch. Ganz im Gegenteil: Es gibt weiterhin bei unterschiedlichen Akteuren das große Interesse, die deutschen Regelungen zur Pflicht zur Benennung von Datenschutzbeauftragten bei nichtöffentlichen Stellen im Rahmen dieser Gesetzgebungsverfahren wieder stark einzuschränken.

Bisheriger Verfahrensgang

Bundesrat

Beide Gesetzentwürfe wurden bereits am 02.10.2018 im federführenden Ausschuss für Innere Angelegenheiten sowie im Wirtschaftsausschuss des Bundesrats beraten. Die Beschlussempfehlung dieser beiden Ausschüsse[3] enthielt zum Entwurf des 2. DSAnpUG-EU auch Vorschläge zur Änderung des BDSG, insbesondere die Streichung oder Abschwächung der Pflicht zur Benennung von Datenschutzbeauftragten für nichtöffentliche Stellen

(Änderungsvorschläge 2 bis 5). Der Bundesrat hat hierüber und über die Änderungsvorschläge der beiden Ausschüsse in seiner Sitzung am 19. Oktober für die erste Runde abschließend beraten und die Änderungsvorschläge zu § 38 Abs. 1 BDSG abgelehnt. Die angenommenen Änderungsvorschläge zu den beiden Gesetzentwürfen finden sich in den Bundesratsdrucksachen 430/18(B)[4] und 433/18(B)[5].

Bundestag

Die erste Beratung im Bundestag ist am 12. Oktober 2018 erfolgt[6]. Es erfolgte – erwartungsgemäß – eine Überweisung an die Ausschüsse, für das 2. DSAnpUG-EU ist der Ausschuss für Inneres und Heimat federführend, für das Datenschutzumsetzung- und -anpassungsgesetz der Ausschuss für Recht und Verbraucherschutz.

Eine – in Bezug auf die Benennungspflicht betrieblicher Datenschutzbeauftragter – wichtige Aussage aus dem Protokoll ist folgende:

Marc Henrichmann (CDU/CSU):
„In den anstehenden Beratungen werden wir noch einige Änderungswünsche besprechen müssen. Da geht es um die Bestellung (sic!) des betrieblichen Datenschutzbeauftragten, die sogenannte Zehner-Schwelle."

Mit Datum vom 31. Oktober 2018 wurde dem Bundestag der Beschluss des Bundesrates und die entsprechende Gegenäußerung der Bundesregierung zum 2. DSAnpUG-EU (Bundestagsdrucksachen 19/5414[7]) und mit Datum vom 07. November 2018 der Beschluss des Bundesrates und die entsprechende Gegenäußerung der Bundesregierung zum Datenschutzumsetzungs- und -anpassungsgesetz EU (Bundestagsdrucksache 19/5554[8]) zugeleitet.

Weiteres Verfahren

Jetzt liegen die Gesetzentwürfe mitsamt Beschlüssen des BR und den Gegenäußerungen der Bundesregierung hierzu in den Ausschüssen des Deutschen Bundestages. Dort werden diese beraten und bei Bedarf Änderungen an den Gesetzentwürfen erarbeitet. Nicht selten kommt es dabei vor, dass die Bundesregierung dem jeweils federführenden Ausschuss eine „Formulierungshilfe" übermittelt, mit der Änderungswünsche der Bundesregierung noch in den Ausschüssen umgesetzt werden sollen. Oft ist es auch schon passiert, dass die entscheidende Sitzung des federführenden Ausschusses am Mittwoch einer Plenarwoche stattfand und dann der Bundestag am Donnerstag oder Freitag der gleichen Woche über den entsprechenden Gesetzentwurf und den vom federführenden Ausschuss vorgelegten Änderungsentwurf in zweiter und dritter Lesung und damit abschließend beraten und beschlossen hat. In solchen Fällen ist es dann selbst für die interessierte Fachöffentlichkeit nicht mehr möglich auf die vorgesehenen Änderungen zu reagieren. Und auch den Abgeordneten im Bundestag ist es kaum möglich sich inhaltlich mit den vorgeschlagenen Änderungen auseinander zu setzen. Da bei



Bild: ClipDealer

dem geplanten Vorhaben mit diesen beiden genannten Gesetzesentwürfen 173 Bundesgesetze geändert werden sollen, gilt dies um so mehr.

Einschränkung der Pflicht zur Benennung von Datenschutzbeauftragten in nichtöffentlichen Stellen?

Die Diskussionen über Änderungen am § 38 Abs. 1 BDSG oder gar dessen vollständige Streichung, die zu einer starken oder gar radikalen Einschränkung einer Pflicht zur Benennung von betrieblichen Datenschutzbeauftragten, also Datenschutzbeauftragten von nichtöffentlichen Stellen führen würden, lassen einen ganz wichtigen Aspekt völlig außer Acht:

Unabhängig davon, ob Verantwortliche und Auftragsverarbeiter Datenschutzbeauftragte zu benennen haben oder nicht, haben die Verantwortlichen und Auftragsverarbeiter alle für sie geltenden Anforderungen der DSGVO umzusetzen.

Dies bedeutet aber auch, dass es bei jedem Verantwortlichen und bei jedem Auftragsverarbeiter eine Person geben muss, die weiß, welche Anforderungen die DSGVO an diesen Verantwortlichen oder Auftragsverarbeiter stellt und wie diese in der Praxis am besten umgesetzt werden können. Welche Geschäftsführung, welcher Vorstand will diese Aufgabe schon selbst übernehmen?

Die Erfahrung in Deutschland zeigt, dass gerade kleinere Unternehmen, die nicht zur Bestellung bzw. Benennung von Datenschutzbeauftragten verpflichtet sind und auch keine Datenschutzbeauftragten benannt haben, sich mit der Umsetzung des Datenschutzrechts schwer tun. Und dies gilt nicht erst seit dem Gültigwerden der DSGVO am 25. Mai 2018 oder der davorliegenden zweijährigen Übergangszeit. Bereits in den Datenschutzzeiten vor der DSGVO – an dieser Stelle sei der Hinweis erlaubt, dass es das erste Bundesdatenschutzgesetz bereits 1977 gab – hatten gerade die Unternehmen, die keine Datenschutzbeauftragten zu bestellen hatten und dieses auch nicht getan hatten, immense Schwierigkeiten, die Anforderungen des alten BDSG umzusetzen. Manch eine Geschäftsführung glaubte sogar (und glaubt vielleicht immer noch) irrigerweise, dass sie sich gar nicht um den Datenschutz kümmern müsste, solange sie keine Datenschutzbeauftragten bräuchte.

Interessant ist an dieser Stelle die Erfahrung des Autors, dass auch kleinere Unternehmen, die nicht verpflichtet wären, Datenschutzbeauftragte zu benennen, dies dann „freiwillig" vornehmen, wenn es plötzlich (meist etwas größere) Auftraggeber gibt, die die Umsetzung des Datenschutzes in diesen kleinen Unternehmen zur Voraussetzung für die Beauftragung von Dienstleistungen erklären, selbst wenn die Verarbeitung personenbezogener Daten des Auftraggebers nicht die Kerntätigkeit dieser kleineren Unternehmen darstellt. Dies zeigt doch, dass die Benennung von Datenschutzbeauftragten die Unternehmen dabei unterstützt, die Anforderungen des Datenschutzes, insbesondere aus der DSGVO, einzuhalten.

Was wäre also dadurch gewonnen, wenn in Deutschland die derzeitigen Regelungen zur Pflicht zu Benennung betrieblicher Datenschutzbeauftragter aufgeweicht oder ganz gestrichen würden, also im Extremfall nur noch die Regelungen aus Art 38 DSGVO zur Benennungspflicht greifen würden? Die Antwort ist einfach: Nichts! Weder für die Unternehmen noch für die betroffenen Personen, deren Daten in den Unternehmen verarbeitet werden.

Um es ganz klar zu formulieren: Wenn die Pflicht zur Benennung betrieblicher Datenschutzbeauftragter aufgeweicht würde, müssten auf der anderen Seite die personellen Ressourcen der deutschen Datenschutz-Aufsichtsbehörden deutlich erhöht werden, da dann – um eine einigermaßen akzeptable Umsetzung des Datenschutzes weiterhin zu gewährleisten – die Kontrolldichte im Bereich Datenschutz enorm erhöht werden müsste. Ist dies wirklich das, was die Unternehmen wollen? Sicher nicht!

Wenn weniger Unternehmen betriebliche Datenschutzbeauftragte benennen, wer soll dann diese Unternehmen bei der Umsetzung des Datenschutzes beraten? Sicher stehen hier viele Rechtsanwältinnen und Rechtsanwälte gerne zur Verfügung. Aber wird dies dann für die Unternehmen einfacher und kostengünstiger? Sicher nicht!

An wen sollen sich denn betroffene Personen wenden, wenn deutlich weniger Unternehmen betriebliche Datenschutzbeauftragte haben? Dann bleiben doch nur die Datenschutz-Aufsichtsbehörden, verbandsklageberechtigte Datenschutzvereine und die Gerichte (unter zu Hilfenahme von Rechtsanwältinnen und Rechtsanwälten). Ist es das, was den betroffenen Personen die Wahrnehmung ihrer Rechte erleichtert und was es den Unternehmen hilft, Datenschutz effizient umzusetzen? Sicher nicht!

Dies soll an dieser Stelle genügen. Weitere Gründe, warum es nicht sinnvoll ist, die in Deutschland bestehenden Pflichten zur Benennung betrieblicher Datenschutzbeauftragten aufzuweichen, finden sich im – auch von der Deutschen Vereinigung für Datenschutz unterstützten – Positionspapier „Wettbewerbsvorteil für deutsche Unternehmen und Schutz von Verbraucherrechten", das auch in dieser Ausgabe abgedruckt ist.

Auszüge aus dem Plenarprotokoll vom 12. Oktober 2018

Vermutlich haben nicht viele das Plenarprotokoll des Bundestags vom 12. Oktober 2018 zum TOP 26[9] (erste Lesung zum 2. DSAnpUG-EU und zum DSUAnpaG-EU) gelesen. Daher wurden hier einige Auszüge ausgewählt. Diese Auszüge verdeutlichen, dass es bei den beiden Gesetzentwürfen mitnichten nur um die Anpassung an die DSGVO und die Umsetzung der JI-Richtlinie geht, sondern dass vielmehr Regelungsvorschläge enthalten sind, die den Datenschutz weiter schwächen.



Bild: Webseite

Marco Wanderwitz, Parl. Staatssekretär beim Bundesminister des Innern, für Bau und Heimat:

„In dem engen Spielraum, den uns die EU-Datenschutz-Grundverordnung hier

lässt, besteht eine der wenigen Möglichkeiten, die es für Erleichterungen gibt, darin, Änderungen an der Bestellpflicht für betriebliche Datenschutzbeauftragte vorzunehmen." (6212 C)

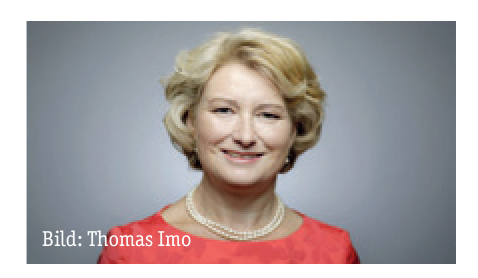


Bild: Thomas Imo

Rita Hagl-Kehl, Parl. Staatssekretärin bei der Bundesministerin der Justiz und für Verbraucherschutz:

„Eine weitere Neuerung ist, dass das Bundesdatenschutzgesetz künftig auch für die Strafverfolgungsbehörden der Länder gelten soll. Damit werden deren Verarbeitungsvorgänge erheblich vereinfacht." (6213 B)

„In Bezug auf die sogenannte zweckändernde Verwendung von Daten aus eingriffsintensiven Maßnahmen, etwa von Telekommunikationsüberwachungen oder Onlinedurchsuchungen, hat der Gesetzentwurf die vom Bundesverfassungsgericht aufgestellten Kriterien aufgegriffen." (6213 B/C)

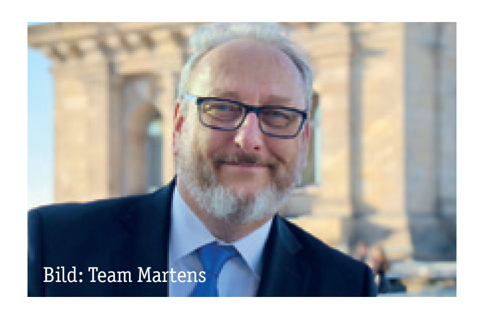


Bild: Team Martens

Dr. Jürgen Martens (FDP):

„Solche Gesetze bringen die fast unwiderstehliche Verlockung mit sich, politisch zumindest schwierige Vorhaben, sagen wir mal, in einem nicht ganz so übersichtlichen Umfeld mit durch das Gesetzgebungsverfahren zu bringen.

Wenn man sich diesen Gesetzentwurf anschaut, stößt man im Bereich des Bundesdatenschutzgesetzes auf einmal in § 22 Absatz 1 Nummer 1d des Bundesdatenschutzgesetzes auf eine zusätzliche Regelung. Da heißt es, dass besonders sensible Daten – solche im Sinne des Artikels 9 der DSGVO – nun auch von nichtöffentlichen Stellen bearbeitet werden können sollen. Das klingt als solches nicht besonders schlimm, aber es stellt sich die Frage: Wer befindet darüber, ob eine entsprechende Datenverarbeitung im öffentlichen Interesse ist oder nicht? Nach Ihrem Gesetz tut das wohl der private Datenverarbeiter. Das dürfte allerdings unzulässig sein, denn: Was im öffentlichen Interesse ist, hat der Gesetzgeber oder zumindest eine öffentliche Stelle zu definieren. Also so einfach, dass es sich hier nur um Anpassungen handelt, ist das Ganze nicht." (6213 D / 6214 A)



Bild: Webseite

Niema Movassat (DIE LINKE):

„Erstens: Die Änderungen im Staatsangehörigkeitsgesetz. Bisher sind Behörden, die mit Staatsangehörigkeitsfragen zu tun haben, die einzigen, die auf die personenbezogenen Daten zugreifen dürfen. Die Übermittlung der Daten an andere Stellen ist per Gesetz nicht erlaubt. Die Bundesregierung will das ändern. Die Daten sollen danach auch an Verfassungsschutzbehörden weitergeleitet werden können, ohne dass ein konkreter Verdacht vorliegt. Das ist kein Datenschutz, sondern eine Datenschutzverletzung.

Zweitens. Sie möchten gravierende Änderungen beim Asylgesetz im Bereich des Datenschutzes vornehmen. Nach der neuen Regelung können das Bundesamt für Migration und Flüchtlinge sowie Ausländerbehörden Gesundheitsinformationen, Berichte über das Sexualleben und andere intime Daten von Geflüchteten an andere Behörden wie die Verfassungsschutzbehörden weiterleiten. Hier wird klar: Datenschutz, selbst der Schutz intimster Daten, soll für Geflüchtete nicht gelten. Das ist abzulehnen; Datenschutz muss für alle gelten.

Drittens. Die Änderungen im Bundesdatenschutzgesetz sehen vor, dass auch nichtöffentliche Stellen Daten für die Sicherheitsbehörden bereithalten müssen. In der Gesetzesbegründung steht: ‚Ein solches zwingendes Erfordernis' – gemeint ist das Erfordernis zur Datenweitergabe – ‚kann etwa bei der Verarbeitung von personenbezogenen Daten mit Religionsbezug durch zivilgesellschaftliche Träger im Rahmen von Präventions- und Deradikalisierungsprogrammen im Bereich religiös motiviertem, insbesondere islamistischem, Extremismus bestehen.' Hiermit werden also zivilgesellschaftliche Organisationen, die wichtige Präventionsarbeit gegen religiöse Radikalisierung leisten, gezwungen, ihre Daten an die Sicherheitsbehörden herauszugeben." (6214 D, 6215 A)

„Aber für den Datenschutz der Betroffenen im Strafverfahren – darum ging es dem Bundesverfassungsgericht eigentlich – haben Sie nicht gesorgt. Vielmehr können nach der neuen Regelung die

Geheimdienste Daten mit den Strafverfolgungsbehörden austauschen. Der Betroffene hat kaum die Möglichkeit, dagegen vorzugehen. Das ist kein Grundrechtsschutz, das ist mehr Macht für die Sicherheitsbehörden.“ (6215 B)



Bild: Webseite

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN):

„Auch mit der zweiten Vorlage schleifen Sie wieder Betroffenenrechte und Aufsichtsmöglichkeiten. An mehreren Stellen werden Abwägungserfordernisse zulasten der Bürgerinnen und Bürger zurückgeschraubt.“ (6215 D)

„Die Koalition aber hat den Gesetzentwurf genutzt, gleich mal etwas mit zu regeln, was dem Datenschutz der Menschen diametral entgegenläuft, nämlich die Erhebung retrograder, aus betrieblichen Gründen von Providern gespeicherter Standortdaten. Das verstecken Sie unter Artikel 1 Ziffer 6 Buchstabe a Unterpunkt bb des Gesetzentwurfs.“ (6215 D, 6216 A)



Foto: Büro Marc Henrichmann

Marc Henrichmann (CDU/CSU):

„In den anstehenden Beratungen werden wir noch einige Änderungswünsche besprechen müssen. Da geht es um die Bestellung des betrieblichen Datenschutzbeauftragten, die sogenannte Zehner-Schwelle. Wir müssen zumindest über Erleichterungen dahin gehend reden, ob es nicht Sinn macht, diejenigen rauszunehmen, die sich nicht schwerpunktmäßig und betrieblich mit Datenverarbeitung befassen.“ (6216 D)



Bild: Webseite

Axel Müller (CDU/CSU):

„Erstens. Die Auffangnorm des § 500 Strafprozessordnung, Frau Staatssekretärin, bedarf durchaus der Erwähnung hier. Sie haben ja gesagt, dort wird klargestellt, dass nunmehr auch bei den Länderbehörden – sprich: bei den Staatsanwaltschaften; Justiz ist ja bekanntlich Ländersache – das Bundesdatenschutzgesetz zur Anwendung kommen soll. Warum eigentlich? Warum kommt nicht das Landesdatenschutzgesetz zur Anwendung? Warum geht das Bundesdatenschutzgesetz dem Landesdatenschutzgesetz vor, wenn Landesbehörden mit Daten umgehen? Wie widersprüchlich die Formulierung ist, zeigt sich in der weiteren Fassung des § 500 StPO. Dort steht nämlich explizit drin, dass für die Einhaltung und Kontrolle der datenschutzrechtlichen Bestimmungen nicht der Bundesdatenschutzbeauftragte, sondern der Landesdatenschutzbeauftragte zuständig ist. Hier ist der Gesetzentwurf widersprüchlich oder unvollständig; es bedarf zumindest einer Korrektur.“ (6218 C)

1 http://dipbt.bundestag.de/dip21/btd/19/046/1904674.pdf

2 http://dipbt.bundestag.de/dip21/btd/19/046/1904671.pdf

3 https://www.bundesrat.de/drs.html?id=430-1-18

4 http://dipbt.bundestag.de/dip21/brd/2018/0430-18B.pdf

5 http://dipbt.bundestag.de/dip21/brd/2018/0433-18B.pdf

6 Vgl. das zu diesem Punkt sehr lesenswerte Plenumsprotokoll http://dipbt.bundestag.de/dip21/btp/19/19056.pdf#P.6211

7 http://dipbt.bundestag.de/dip21/btd/19/054/1905414.pdf

8 http://dipbt.bundestag.de/dip21/btd/19/055/1905554.pdf

9 http://dipbt.bundestag.de/dip21/btp/19/19056.pdf#P.6211

Joachim Jakobs

Was nur wenige wissen: Datenschutzfolgenabschätzungen sind für viele Anwendungen Pflicht!



Bild: iStock

Hundert Terabytes benötigen per LTE (300 MBit/s) 31 Tage zur Übertragung – eine Übung, die sich per 5G (1 GBit/s) auf knapp 10 Tage reduziert. Künftig wollen wir aber Daten in Bakterien speichern und über Petabit-Leitungen übertragen, um so personalisierte Prothesen, menschliche Organe, Medikamente, Lebensmittel, Kleidung, Möbel, Autos/Häuser (aus der Ferne) in 3D zu drucken, Lohnabrechnungen per RFID und videobasierte Persönlichkeitsprofile in Echtzeit zu erstellen oder mit der Genschere CRISPR am Erbgut rumzufummeln. 3D-Echtzeitrekonstruktionsverfahren ermöglichen die natürliche Kommunikation örtlich getrennter GesprächspartnerInnen – so werden Wissenschaft, Forschung und Lehre umgekrempelt. Auch Banken, Energieversorger, Stadtverwaltungen, Telekommunikationsunternehmen und (Sozial-) Versicherungen stehen vor der digitalen Transformation: Vom alltäglichen Beschwerdemanagement bis zur zukunftsorientierten Vertriebssteuerung – überall können Entscheidungen, die bisher mit Erfahrung und einer gesunden Portion Bauchgefühl getroffen wurden, durch stetig wachsende Datenbestände, ausgeklügelte Algorithmen und Künstliche Intelligenz (KI) gestützt oder gänzlich automatisiert werden. Die KI soll für steuerberatende Berufe alle umsatzsteuerrelevanten Daten auswerten und strukturieren, so dass die Angaben aus allen Datenquellen automatisiert auf Knopfdruck zur Umsatzsteuervoranmeldung genutzt werden können. Ein Roboter-Anwalt soll bereits menschliche KollegInnen ersetzen. Zur Vernetzung der Welt stehen uns 350 Sextillionen IP-Adressen zur Verfügung. Damit ließen sich die 100 Billionen Körperzellen von theoretisch 10 Milliarden ErdenbürgerInnen 350.000mal durchnummerieren. Die Zeit, um die (unbeabsichtigte und evtl. unrechtmäßige) Übertragung des oben genannten Datenvolumens abzubrechen, würde sich mit einer Petabit-Leitung auf eine Sekunde reduzieren.

Die Kehrseite der Medaille – auch auf der kriminellen Seite tut sich Einiges: Je breitbandiger die Netzverbindungen, desto massiver die möglichen Konsequenzen von Überlastungsangriffen. Schlimmer noch: Kriminelle künstliche Intelligenz erteilt wahlweise Empfehlungen, bei welcher IP-Adresse ein Angriff lohnt – oder führt diesen Angriff auf Wunsch auch grad noch autonom durch. Ziel auswählen – fertig!

Von Betroffenen werden bereits heute hohe Summen bezahlt, damit deren Gesundheitsakte nicht im Internet veröffentlicht wird. Wieviel sind Sie bereit dafür zu bezahlen, dass niemand an Ihren elektronischen Innereien rummacht? Und: Werden Sie mit diesen Innereien zum Risiko für Ihren Arbeitgeber? Bis 2021 wird damit gerechnet, dass die Cyberkriminalität weltweit 6 Billionen (!) US-$ jährlich erwirtschaftet. Unklar ist dabei, ob in diesem Betrag die künftige Leistungsfähigkeit von neuen Anwendungen bereits berücksichtigt ist oder ob dadurch die Beute noch erhöht wird. Der russische Präsident Wladimir Putin ist jedenfalls der Ansicht, wer die KI beherrsche, beherrsche die Welt.

Bislang drücken wir uns vor der Debatte, ob wir beherrschen was wir tun und was das alles für uns bedeutet: Gesundheitsminister Jens Spahn möchte die elektronische Patientenakte per „Smartphone" zugänglich machen. Sinnvoll wäre es jedoch erst einmal, die Patientenakte, das schlaue Telefon und alle anderen an diesem System beteiligten Hard- und Softwarebausteine zwischendrin zunächst einem unabhängigen Pentest (Penetrationstest) zu unterziehen.

Haften müssen die Verantwortlichen. In der Wissenschaft könnte beispielsweise Wolfgang Wahlster, Geschäftsführer vom Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) in Saarbrücken, zu dieser Spezies zählen. So ist es denkbar, dass etwa im Forschungsprojekt „Human Analytics Apps TrackMe und GeoVisualizer" personenbezogene Daten verarbeitet werden: Bereits auf der Cebit 2014 soll gezeigt worden sein, wie Vitalparameter, Emotionen, Aktivitäten und personenbezogene Daten wie Geschlecht oder Alter mit Informationen aus der unmittelbaren Umgebung in Verbindung gebracht werden können. Solche Vitalparameter könnten für „Generali Vitality" verlockend sein – der Versicherungskonzern will seine KundInnen „für jeden Schritt in ein gesünderes Leben" belohnen. Bislang hat sich die DFKI-Pressestelle jedenfalls nicht dazu geäußert, ob das Institut tatsächlich in irgendeinem seiner 240 Forschungsprojekte mit realen personenbezogenen Daten arbeitet oder stattdessen Testdaten nutzt. Bei diesen Projekten mit personenbezogenen Daten wäre derjenige, der über die Mittel und Zwecke der Datenverarbeitung entscheidet, für die Einhaltung von Artikel 5 Absatz 1 der Datenschutzgrundverordnung (DSGVO) „verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht")" (Artikel 5 Abs. 2 DSGVO).

Zur Rechenschaftspflicht gehört auch die „Sicherheit der Verarbeitung"; in Artikel 32 DSGVO schreibt der Gesetzgeber: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten." Das bedeutet: Der Verantwortliche ist verpflichtet, die Eintrittswahrscheinlichkeit und Schwere von Risiken systematisch zu erfassen, zu bewerten und daraus das angemessene Schutzniveau abzuleiten. Dieses Schutzniveau muss dann durch die technischen und organisatorischen Maßnahmen (TOM) auf dem „Stand der Technik" erreicht werden. Das Bundesjustizministerium definiert den Begriff so: „Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen [...] müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein." Der Regierung ist also das Beste grade gut genug, was der Markt an TOM hergibt.

Sollte sich bei der Risikoanalyse herausstellen, dass die „Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge" hat, „so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch" (Artikel 35 Abs. 1 S. 1 DSGVO).

Eine Datenschutzfolgenabschätzung (DSFA) ist dem Gesetzgeber besonders bei der systematischen und umfassenden „Bewertung persönlicher Aspekte natürlicher Personen" wichtig, „die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen" (Artikel 35 Abs. 3 lit. a DSGVO). Solche Entscheidungen könnten womöglich in Belohnungen bestehen, wie sie Generali Vitality verspricht.

Die DSFA enthält dem Gesetzgeber zufolge „zumindest Folgendes:

a. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen [...] und

d. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird" (Artikel 35 Abs. 7 DSGVO).

Verantwortliche sind auf verschiedenen Ebenen rechenschaftspflichtig: Ein Projektverantwortlicher muss diesem Anspruch in seinem Projekt gerecht

werden. Und z. B. DFKI-Geschäftsführer Wolfgang Wahlster muss dafür sorgen, dass seine ProjektleiterInnen von ihrer Rechenschaftspflicht überhaupt Notiz nehmen. Die Nicht-Kenntnisnahme entschuldigt den Projektleiter nicht; das einzige Schlupfloch: „Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung [...] befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Artikel 82 Abs. 3 DSGVO). Der TÜV Nord warnt: „Datenschutz: Ab 2018 haften Geschäftsführer in Millionenhöhe".

Zusammengefasst verlangt die DSGVO nach „Sicherheit 4.0". Das bedeutet: Wir müssen – flächendeckend, systematisch, proaktiv – investieren in Sicherheits-/Notfallkonzepte, physikalischen Einbruchschutz, elektronische Signaturen, kryptographische Verschlüsselungen, IAM-/SIEM-Systeme, rollenspezifische Bildung für Alle, herstellerunabhängige (nach Möglichkeit dynamische) Gütesiegel für die Wolke sowie Produkte/Dienstleistungen/"Apps" und Penetrationstests.

Dabei bitte den Stand der Technik nicht vergessen – vielfach ist das KI, denn KI soll auch Wege finden, die dem Menschen auf den „ersten Blick" verborgen bleiben. Je früher die Verantwortlichen die Zusammenhänge verstehen, desto billiger wird es!

Mehr noch: Wir müssen den ebenfalls durch die digitale Transformation betroffenen HandwerkerInnen und FreiberuflerInnen samt deren Personal die Zusammenhänge erklären. Unklar ist allerdings, woher wir die Ressourcen nehmen sollen, um die Millionen Menschen in der mittelständischen Wirtschaft über die Zusammenhänge und ihre sich daraus ergebenden Pflichten aufzuklären.

Sicher ist nur: Die technische Entwicklung geht weiter. Claus Cristian Timmermann, Professor für Nachrichtentechnik, denkt über „ExaBit/s" nach. Dadurch würde sich die Zeit zur Übertragung von 100 Terabytes wohl auf eine tausendstel Sekunde reduzieren.

Der Autor hat 2015 „Vernetzte Gesellschaft. Vernetzte Bedrohungen. Wie uns die künstliche Intelligenz herausfordert" veröffentlicht.

Kathrin Häring und Holger Nohr[1]

Regulierung des Datenschutzes für Kinder

Zusammenfassung

Soziale Medien sind fester Bestandteil des Alltags vieler Kinder und Jugendlicher. Mit der steigenden Nutzung solcher Medien steigen auch Anforderungen an das Datenschutzrecht, ebenso wie die Herausforderungen an den bewussten Umgang mit persönlichen Daten. Besonders Kinder, die soziale Medien mit einer Selbstverständlichkeit nutzen und zum Teil unbewusst Daten über sich und andere preisgeben, bedürfen besonderen Schutz, denn von ihnen kann kein verständiger Umgang mit personenbezogenen Daten erwartet werden. Der Beitrag begründet die besondere Schutzwürdigkeit von Minderjährigen in datenschutzrechtlicher Hinsicht und gibt einen Überblick über die relevanten Regeln der EU-Datenschutz-Grundverordnung (DSGVO) bzgl. Minderjähriger.

I. Einleitung und Relevanz

Fernsehgeräte/Smart-TVs, Smartphones/Handys, Computer/Laptops und Internetzugang sind in nahezu allen deutschen Haushalten (mindestens je 97%) vorhanden und für Kinder alltäglich. Kinder wachsen selbstverständlich mit digitalen Medien auf und – so eine Annahme – verstehen nicht hinreichend, dass vielfältige personenbezogene Daten bei der Nutzung der Geräte und Dienste erhoben werden und welche Risiken daraus resultieren[2]. Erste Ergebnisse aus unserem Projekt zum „Datenschutzbewusstsein bei der Social-Media-Nutzung von Kindern und Jugendlichen"[3] bestätigen diese Annahme. So sind auf Plattformen wie Instagram und Snapchat die Story-Funktionen beliebt, bei denen Daten geteilt werden, die auf den ersten Blick nur 24 Stunden für andere Nutzer sichtbar sind. Eine vermeintlich sichere Art, Daten von sich zu teilen, denen Kinder Vertrauen schenken, wie unsere Gruppendiskussionen mit Schülerinnen und Schülern unterschiedlicher Bildungsniveaus zeigen. Viele Kinder gehen davon aus, dass Liken und Kommentieren der Inhalte anderer, sowie die Nutzung einer solchen Story-Funktion bedenkenlos sei, weil keine Spuren hinterlassen würden. Sie lassen dabei außer Acht, dass die Daten bei den Plattformbetreibern gespeichert bleiben und von diesen etwa zur Profilbildung genutzt werden. Dieser unaufmerksame und uninformierte Umgang mit Daten stellt ein klassisches Problem der Nutzung von Social-Media-Diensten dar, die von einer Selbstthematisierung und dem Teilen persönlicher Inhalte leben. In diesem Kontext spielen datenbasierte Geschäftsmodelle und eng mit diesen verbunden, die Auswertung großer Datenmengen mit Big Data eine zentrale Rolle. Kinder können nur schwer und vereinzelt einschätzen, wie schnell und vergleichsweise einfach sie etwa durch ihr Smartphone abgehört werden können oder welche Folgen solche Aktionen haben können. Die Sicherheitslücke „Stagefright", welche Mitte 2015 öffentlich bekannt wurde, erlaubt es Angreifern durch einfache technologische Manipulation wie einem Exploit-Code in einer MMS an das Smartphone des Betroffenen, dieses „Smartphone in eine Wanze zu verwandeln, die Kamera anzusteuern, die Mediengalerie auszulesen, auf die Bluetooth-Schnittstelle zuzugreifen oder auch weiteren Schadcode wie etwa Keylogger nachzuladen[4].


Bild: iStock

Kindern digitale Medien vorzuenthalten, ist jedoch keine Alternative. Kinder müssen die Möglichkeit haben, eigene Erfahrungen zu sammeln und auf diese Weise zu lernen. Sie sollten dabei Zugang zu Medienbildungsangeboten haben, um sich selbst weiterzubilden. Wie aus unseren Gruppendiskussionen hervorgeht, nutzen viele 14- und 15-Jährige etwa die Plattform Youtube, um sich Themen, die sie in der Schule nicht verstanden haben, auf andere Weise erklären zu lassen. Im Unterschied zu anderen schutzbedürftigen Personen sind Kindern auf einer Entwicklungsstufe, auf der selbstbestimmtes Handeln noch erlernt wird und nicht vorausgesetzt werden kann.

Zahlen der aktuellen KIM-Studie zeigen, dass viele Nutzer gegen die Altersbedingung der AGBs von meist 13 Jahren verstoßen. Viele Kinder haben das Mindestalter vor der Nutzung nicht erreicht. In der KIM-Studie werden elterliche Regelungen für die Nutzung meist ab ca. zwölf Jahren ermittelt (YouTube: 11,3 Jahre, WhatsApp: 11,4 Jahre, Snapchat: 12,7 Jahre). Die Realität sieht hingegen anders aus: 26% der 6- und 7-Jährigen sind bereits WhatsApp-Nutzer, unter den 8- und 9-Jährigen sind es sogar 36%, ab 10 Jahre nutzen den Messenger sogar über die Hälfte der befragten Kinder. [5]

Kinder zählen zu den häufigen Nutzern von Online-Netzwerken und damit zu denen, die dazu neigen, unüberlegt Daten öffentlich zu teilen. Kinder besitzen bereits in jungen Jahren ein eigenes Smartphone und nutzen dieses häufig mit Internetzugang aber ohne inhaltliche Eingrenzung, obwohl für die Hauptfunktion – die Kommunikation vor allem mit den Eltern –, die oft den Kauf eines solchen Geräts rechtfertig, ein Mobiltelefon ausreichen würde. Für Kinder allerdings stellt dieser Grundgedanke nicht mehr die meistgenutzte bzw. beliebteste Funktion dar, sie nutzen die Geräte vor allem als Unterhaltungsmedium und zur Kommunikation mit Freunden, Bekannten oder Fremden. Kommunikation hat sich verändert und ausgeweitet, sodass viele Gespräche, die nicht zwingend über solche Geräte stattfinden müssten, auf die digitale Kommunikation verschoben werden. Vor allem des Unterhaltungsfaktors wegen sind Smartphones, sowie andere mobile internetfähige Geräte bei Kindern, die meist auch in sozialen Netzwerken aktiv sind, sehr beliebt. Das Teilen privater Inhalte und persönlicher Informationen beschreibt einen unverzichtbaren Bestandteil der Geschäftsmodelle sozialer Netzwerke, die für Kinder kaum durchschaubar sind. „Im Internet werden heute immer mehr Daten verbreitet, die klassischerweise mit der Welt des Intimen, Privaten, Geheimen oder (auch nur) Alltäglichen assoziiert werden“.[6] Eine Einwilligung der Eltern und damit die Erlaubnis, Kinder frei in sozialen Netzwerken agieren zu lassen, wie sie bisher vermutlich eher selten tatsächlich eingeholt wurde, fordert entsprechendes Vertrauen in eine verantwortungsbewusste Nutzung und notwendige Reife. Dabei neigen Eltern oft dazu, ihren Kindern zu viel zuzutrauen oder die Nutzung zu erlauben, um sie vor anderen Kindern nicht auszugrenzen. Kinder, die in sozialen Netzwerken nicht aktiv sind, stellen eine Minderheit dar und grenzen sich damit aus manchen Kommunikationen aus. Kinder sind einerseits wenig interessiert an der Weiterverarbeitung ihrer Daten, andererseits ist es für sie schwer nachvollziehbar, welche Daten wie und wofür weiterverwendet werden[7] und dass nicht nur aktiv und bewusst geteilte Daten (z. B. Bilder) erhoben und genutzt werden.

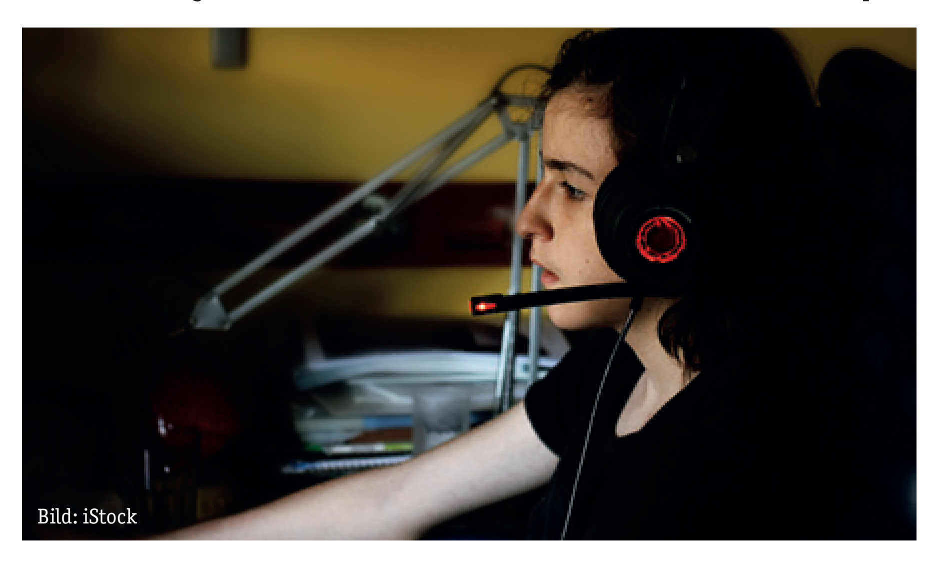
Nie zuvor wurden so viele Daten erhoben und analysiert, was bedeutet, dass von Kindern, die heute mit digitalen Medien aufwachsen, von klein auf Massen von Daten erhoben werden, mit unvorhersehbaren Auswirkungen auf die Entwicklung dieser Generation. Kinder tragen hier die Konsequenzen der Datenverarbeitung am stärksten und am längsten[8], wodurch das Prinzip der Datensparsamkeit an Bedeutung gewinnt. Wenn auch die Nutzung digitaler Medien Potentiale besitzt, wirft der Umgang mit solchen Medien und Big Data neue ethische Fragen auf für die Erhebung und Verarbeitung personenbezogener Daten, sowohl von Kindern, als auch von Erwachsenen[9]. Speziell stellt sich die Frage, welche Daten für welche Zwecke erhoben werden dürfen und in welchem Rahmen diese Daten von Unternehmen genutzt werden dürfen. Auf Nutzerprofile abgestimmte und gezielt geschaltete Werbung wur-

de in den vergangenen Jahren gängig und wird obwohl sie einer bewussten Manipulation gleicht, von vielen Nutzern toleriert. Kinder, die noch nicht in der Lage sind zu rekonstruieren woher welche Werbung kommt und dass diese ganz bewusst durch eigenes Verhalten in der Vergangenheit ausgelöst wurde, sollten vor solchen Absichten geschützt sein. Kinder sind wesentlich einfacher beeinflussbar, weil ihnen die technischen Hintergründe und Algorithmen nicht bekannt sind oder sie solche nicht verstehen. Livingstone wirft die Frage auf, ob die digitale Welt den Rechten von Kindern gerecht werden kann und wie sie auch Möglichkeiten für verletzliche und benachteiligte Personen öffnen kann. Dabei steht nicht die digitale Lebenswelt gegen fundamentale Rechte, vielmehr gilt es, die digitale Welt zu nutzen, um Kindern über ihre eigenen Rechte aufzuklären und sie auf die eigenen Rechte aufmerksam zu machen[10]. Nicht nur wann Eltern und Staat wofür Verantwortung übernehmen müssen, sondern wie sich verschiedene Rechte nicht gegenseitig widersprechen, definiert die Herausforderung. Kinder haben einerseits das Recht auf Bildung, auf Information und Medien ihrer Wahl und andererseits auf Privatsphäre und den Schutz vor Gewalt und auf die Freiheit sich auszudrücken. Wie kann der Schutz, auf den Kinder ein Recht haben, gewährleistet werden, während ihnen auch die Freiheit gegeben werden soll, die ihnen zusteht?[11]

Wie bedeutsam und ausbaufähig in diesem Kontext der Datenschutz für Kinder ist, belegt etwa der Annual Privacy Sweep 2015 des Global Privacy Enforcement Network[12]: Aus den Ergebnissen geht u. a. hervor, dass auf den untersuchten Webseiten und Apps viele datenschutzbezogene Texte für Kinder unverständlich sind und überarbeitet werden müssten. Auf vielen Seiten werden zu viele Daten gesammelt, die nicht gesammelt werden müssten. Laut der Pressemitteilung des GPEN 2016 wurden rund 60% der Nutzer nicht ausreichend über die Datenerhebung informiert, ebenso nicht darüber, wie Daten weiterverarbeitet werden. 67% der untersuchten Websites/Apps sammeln persönliche Daten von Kindern. Lediglich 31% verfügten über wirksame Kontrollen, um die Erfassung personenbezogener Daten von Kindern einzuschränken.

II. Die EU-Datenschutz-Grundverordnung und ihre Regelungen für Kinder

Der Schutz von Kindern nimmt – anders als im bisherigen BDSG – in der EU-Datenschutz-Grundverordnung eine wichtige Rolle ein[13] und stellt im deutschen Datenschutzrecht ein Novum dar[14]. Das neue Datenschutzrecht reagiert so auf die eingangs beschriebenen Entwicklungen und Herausforderungen. Regelungen für den Datenschutz speziell für Kinder (Minderjährige) sind in die DSGVO integriert und finden sich an verstreuten Fundstellen, z. T. in den Erwägungsgründen (Tabelle 1 enthält eine Übersicht der Fundstellen). Anders als in den USA, wo mit dem Children's online Privacy Protection Act (COPPA)[15] für die Altersgruppe unter 13 Jahren eine detailreiche und spezifische Vorschrift vorliegt, die etwa die Datenerhebung, das Tracking, die Einwilligung der Eltern (und ihre Form) oder Informationspflichten und Auskunftsrechte regelt.


Bild: iStock

Die zentrale Aussage und Begründung zur besonderen Schutzwürdigkeit von Kindern und ihren personenbezogenen Daten enthält die DSGVO im ErwG 38:

„Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein."

Auf den Schutz der Privatsphäre von Kindern im Internet – wie sie die Kinderrechtskonvention der UN in Art. 16 fordert – wurde vor der Neuregelung in keinem Gesetz speziell eingegangen, das BDSG (alt) berief sich auf die Einsichtsfähigkeit der Nutzer, die von Kindern nicht erwartet werden könne. Der Bundesgerichtshof stellte bereits im Jahr 2014 fest[16]: „Es könne nicht davon ausgegangen werden, dass Minderjährige ab dem 15. Lebensjahr grundsätzlich bereits die nötige Reife hätten, die Tragweite einer Einwilligungserklärung zur Datenspeicherung und -verwendung für Werbezwecke zu erkennen." Minderjährige können ihre Persönlichkeitsrechte in dem Maße wahrnehmen, wie sie zur Einsicht in die Bedeutung dieser Rechte fähig sind. Die Dynamik jedes Entwicklungsprozesses bedingt, dass die Einsichtsfähigkeit grundsätzlich nicht abstrakt, sondern jeweils nur konkret und individuell vorgenommen werden kann[17]. Deshalb müsste eigentlich in jedem Einzelfall beurteilt werden, ob ein Minderjähriger die Bedeutung der Weitergabe seiner Daten versteht und sich auf dieser Basis selbst für eine Preisgabe entscheiden kann.

Thema	DSGVO		BDSG (neu)
Besonderer Schutz der Daten von Kindern		ErwG 36	
Risiken für die Rechte und Freiheiten natürlicher Personen		ErwG 75	
Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft	Art. 8	ErwG 38	
Rechtmäßigkeit der Verarbeitung – berechtigtes Interesse	Art. 6 Abs. 1 lit. f		
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person	Art. 12 Abs. 1	ErwG 58	
Recht auf Löschung (insbes. Kinder, ggf. nach Volljährigkeit)	Art. 17 Abs. 1 lit. f	ErwG 65	
Profiling		ErwG 71	
Aufgaben der Aufsichtsbehörden	Art. 57 Abs. 1 lit. b		§ 14
Verhaltensregeln	Art. 40 Abs. 2 lit. g		

Tabelle 1: Kinder-relevante Fundstellen in der DSGVO

Mit stetigem Zuwachs der Nutzung von Social-Media-Diensten hat auch eine solche Nutzung durch Kinder unter 16 Jahren anhaltend zugenommen. Die Anbieter haben sich dabei bisher über die Zustimmung ihrer Nutzungsbedingungen abgesichert und dabei mit einem Mindestalter von 13 Jahren agiert (wobei diese Altersgrenze durch eine falsche Angabe des Geburtsdatums leicht zu umgehen war, siehe oben die Ergebnisse der KIM-Studie). Seit der Gültigkeit der DSGVO haben erste Anbieter (z. B. WhatsApp, Instagram oder Twitter) ihre Altersgrenze in den letzten Wochen bereits auf 16 Jahre angehoben[18] und auch Accounts jüngerer Minderjähriger gelöscht.

Grundsätzlich bleibt in der DSGVO das „Verbotsprinzip mit Erlaubnisvorbehalt" bestehen[19]. Damit ist eine Verarbeitung personenbezogener Daten nur dann zulässig, wenn einer der in Art. 6 der DSGVO benannten Erlaubnistatbestände vorliegt.

Einer der für Unternehmen gangbaren Erlaubnistatbestände ist die Einwilligung, deren Bedingungen generell in Art. 7 DSGVO geregelt sind. Dieser Erlaubnistatbestand erhält nun allerdings für die Personengruppe der Kinder und in Bezug auf die sog. Dienste der Informationsgesellschaft in Art. 8 eine gesonderte Regelung, die die besondere Schutzwürdigkeit und eine ggf. noch nicht hinreichend ausgeprägte Einsichtsfähigkeit umzusetzen versucht. Eine Einwilligung ist danach nur rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat; bei diesen Minderjährigen wird die erforderliche Einsichtsfähigkeit angenommen[20]. Bei jüngeren Kindern ist eine Einwilligung durch den Träger der elterlichen Verantwortung für das Kind erforderlich oder dessen Zustimmung, realisierbar z. B. über ein double opt-in.

Für die Bestimmung eines Dienstes der Informationsgesellschaft wird in Art. 4 der DSGVO auf die EU-Richtlinie 2015/1535 verwiesen, wonach „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" gemeint ist. Diese Angebote sollen „einem Kind direkt gemacht" werden. Dabei darf wohl davon ausgegangen werden, dass nicht nur ausschließlich an Kinder gerichtete Angebote gemeint sind, sondern dass ebenfalls Angebote, die sich auch an Kinder (neben Erwachsenen) richten, diesen Bedingungen unterstehen.

Hinsichtlich der Altersgrenze enthält Art. 8 Abs. 1 eine Öffnungsklausel für die Mitgliedsstaaten. Diese können eine niedrigere Altersgrenze festlegen, die das vollendete dreizehnte Lebensjahr nicht unterschreiten darf. Diese Öffnungsklausel haben Mitgliedsstaaten

für unterschiedliche Festlegungen zwischen 13 und 16 Jahren genutzt, womit in diesem Punkt eine EU-weite Harmonisierung leider kaum stattfindet[21]. Deutschland hat diese Öffnungsklausel nicht genutzt. Zur Sicherstellung, dass tatsächlich ein Erziehungsberechtigter einwilligt, verlangt die DSGVO in Art. 8 Abs. 2 vom Verantwortlichen angemessene Maßnahmen „unter Berücksichtigung der verfügbaren Technik", die im Rahmen der Kontroll- und Nachweispflichten auch zu belegen sind. Ob ein Alterscheck, wie ihn WhatsApp einführen will, hinreicht – Nutzer sollen ihr Alter bestätigen, eine Kontrolle soll hingegen nicht stattfinden – darf bezweifelt werden.

Ein weiterer Erlaubnistatbestand ist die Verarbeitung im berechtigten Interesse des Verantwortlichen – der Auffangtatbestand der DSGVO[22]. Diese erfordert eine Abwägung, denn sie greift nur, sofern nicht die schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Die dafür erforderliche Interessensabwägung ist immer dann besonders sorgfältig durchzuführen, „wenn es sich bei der betroffenen Person um ein Kind handelt" (DSGVO Art. 6 Abs. 1 lit. f). Dabei ist dem Schutzbedürfnis von Kindern in besonderem Maße Rechnung zu tragen[23].

Weitere spezielle Regeln und Hinweise – spezifisch ausgerichtet auf die Verarbeitung von Daten von Kindern – finden sich unter den Transparenz- und Informationspflichten sowie den Rechten der Betroffenen. Die Informationspflichten müssen nach Art. 12 Abs. 1 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitgestellt werden. Dem folgt die Aussage, dass dies insbesondere für Informationen gilt, die sich speziell an Kinder richten. Eine Erläuterung wird in ErwG 58 gegeben, der mit Bezugnahme auf die besondere Schutzwürdigkeit von Kindern Informationen und Hinweise fordert, die in einer klaren und einfachen Sprache gegeben werden, so „dass ein Kind sie verstehen kann".

Unter den Rechten der Betroffenen wird indirekt Kindern bezüglich dem „Recht auf Vergessenwerden" (Art. 17 DSGVO) und damit der Löschung von Daten insbes. dann ein besonderer Stellenwert zugeschrieben (ErwG 65), wenn eine Einwilligung noch im Kindesalter erfolgt ist und insofern die betroffene Person „die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte".

Wichtig ist zudem, dass die DSGVO verlangt, dass von Verarbeitungen, die als automatisierte Einzelentscheidungen einschließlich Profiling[24] (Art. 22 DSGVO) gelten und in ErwG 71 näher erläutert werden, kein Kind betroffen sein sollte (ErwG 71). Ob diese Aussage als generelles Verbot der Anwendung von Big Data-Methoden auf Kinder ausgelegt werden kann bzw. in welchen konkreten Fällen eine diesbezügliche Einschränkung gilt, muss letztlich offen bleiben. Der Europäische Datenschutzausschuss (European Data Protection Board) vertritt in seinen Leitlinien[25] nicht die Ansicht, dass diese Aussage ein absolutes Verbot einer solchen Art der Verarbeitung in Bezug auf Kinder darstellt. In Anbetracht der Erwägungen im ErwG 71 empfiehlt der Ausschuss jedoch, sich nicht auf die Ausnahmen in Art. 22 Abs. 2 zu berufen, um eine solche Verarbeitung in Bezug auf Kinder zu rechtfertigen, außer wenn dies etwa zum Schutz ihres Wohlergehens geschieht. Der für die Verarbeitung Verantwortliche hat in diesen Fällen für Kinder geeignete Schutzmaßnahmen zu treffen und sicherzustellen, dass diese Maßnahmen die Rechte, Freiheiten und berechtigten Interessen der Kinder wirksam schützen.

Risiken für die Rechte und Freiheiten natürlicher Personen können aus verschiedenen – in ErwG 75 benannten – Verarbeitungen personenbezogener Daten hervorgehen. In diesem Kontext werden schutzbedürftige natürliche Personengruppen genannt, insbes. Kinder. Der Europäische Datenschutzausschuss führt daraus abgeleitet in seinen Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)[26] unter den Kriterien, die als Anhaltspunkt für die Durchführung einer DSFA zu prüfen sind, solche schutzwürdigen Personengruppen auf und nennt ausdrücklich auch Kinder (mit dem Zusatz: „bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen").

Die DSGVO gibt Verbänden und anderen Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, die Möglichkeit Verhaltensregeln ausarbeiten, mit denen die Anwendung der Verordnung präzisiert wird. Dabei wird u. a. „Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist" genannt (Art. 40 Abs. 2, lit. g DSGVO).

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wird in § 14 BDSG (neu) verpflichtet, die Öffentlichkeit für Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären und dabei insbesondere spezifische Maßnahmen für Kinder zu treffen.

III. Diskussion

Die Verbreitung digitaler Medien führt zu einer kaum vermeidbaren flächendeckenden Mediatisierung des Alltags. Viele Vorgänge benötigen dabei personenbezogene Daten, erheben jedoch – oft weitgehend unbemerkt – weitere, für den eigentlichen Zweck nicht notwendige Daten. Während sich Technik stetig entwickelt, hält die Entwicklung des Bewusstseins der Nutzer kaum Schritt. Wann und wie Daten gesammelt werden oder dass dies überhaupt geschieht, ist vielen Nutzern kaum in vollem Umfang bewusst. Vor allem Kinder wissen zwar, wie sie soziale Netzwerke nutzen können, wie sie Freunde und Bekannte finden und auf Inhalte stoßen, die ihnen gefallen, wie sie mit anderen Nutzern in Kontakt treten oder Inhalte teilen können. Allerdings scheinen gerade auch junge Nutzer sich möglicher Konsequenzen wenig bewusst zu sein. „Bereits wenige vorhandene Daten wie das Klickverhalten eines Nutzers können Auskunft über zum Teil sehr sensitive Informationen zur sexuellen oder politischen Einstellung geben."[27]

„Selbstdatenschutz umfasst sowohl den Einsatz von PET (z. B. Pretty Good Privacy (PGP)-Verschlüsselung, Nutzung des Tor-Netzwerks, Cookie-Blocker) als

auch allgemein taktisches Handeln (Vermeidung bestimmter digitaler Dienste und Medien), kulturelles Umdenken sowie den Erwerb medientechnischer Kompetenzen. Individuen sollen in die Lage versetzt werden, Risiken im Umgang mit Informationstechnologien selbst einschätzen sowie alle erforderlichen Maßnahmen treffen zu können, um dem Risiko, überwacht zu werden, so weit als möglich zu entgehen."[28] Dass Kinder durch die Entwicklung der sozialen Medien und vermehrte Mediennutzung eines besonderen Schutzes bedürfen, scheint ein logischer Schluss – durch eine weniger stark ausgeprägte Urteils- und Einsichtsfähigkeit, die Kinder mitbringen[29], sollte ihnen nicht die alleinige Verantwortung bei der Mediennutzung übertragen werden. Der Datenschutz muss diesem Umstand Rechnung tragen und durch entsprechende Regulierung in gewissem Grade einen Schutz für Kinder gestalten. Das neue Datenschutzrecht der EU ist in diesem Sinne tatsächlich ein Fortschritt bei der angemessenen Gestaltung von Kinder- und Jugendrechten im digitalen Zeitalter[30]. Hinter den punktuellen Vorschriften steht allerdings ersichtlich kein Gesamtkonzept[31]. So wird ansatzweise zwar die Forderung nach Schutz der Privatsphäre in Art. 16 der UN-Kinderrechtskonvention abgebildet, ob hingegen mit der o. g. Einwilligungsregelung der Kindeswillen angemessen berücksichtigt (Art. 12 Kinderrechtskonvention) wird, bleibt dahingestellt.

Auch spezifische Fragen bleiben auch nach Einführung der DSGVO bestehen. Eine zentrale Frage betrifft die praktische Umsetzung der Regelung, dass Minderjährige das 16. Lebensjahr beendet haben müssen, um Social-Media-Dienste nutzen zu dürfen. Wie kann sichergestellt werden, dass die Kinder entweder alt genug sind oder tatsächlich ihre Eltern die Einwilligung für Kinder unter 16 Jahren erteilt haben? Hier fehlen klare und rechtssichere Vorgaben.

Persönliche Informationen von Kindern werden im Netz häufig von Eltern geteilt. Einen wirksamen Schutz der Kinder vor dieser elterlichen Verletzung der Privatsphäre leistet das EU-Datenschutzrecht nicht.

Zudem sollte in der Forschung intensiver der Frage nachgegangen werden, wann Kinder wirklich die Einsichtsfähigkeit besitzen, um Social-Media-Dienste eigenständig zu nutzen. Wohl kaum ist dies an einem bestimmten Alter pauschal für alle Kinder bestimmbar. Kinder entwickeln in unterschiedlichem Alter die nötige Einsichtsfähigkeit und die Reife, die es braucht, um mögliche Konsequenzen einer Datenverarbeitung abschätzen zu können. Je nach Entwicklung des Kindes und der betroffenen Daten müsste individuell entschieden werden, wann Kindern eine eigenständige Nutzung zugetraut werden kann[32]. Dabei ist einerseits das Verwehren des Zugangs in Bezug auf soziale Ausgrenzung zu beachten, andererseits die Gefahr durch Unwissenheit Daten zu teilen, die im späteren Leben zu ungeahnten Konsequenzen führen können. Zudem scheint eine Altersgrenze von 16 Jahren im Zeitalter der Digitalisierung kaum zeitgemäß und umsetzbar. Eine Art Vorstufe wäre dabei hilfreich, wobei vermutlich die Eltern tiefer einbezogen werden müssten, was die Umsetzung erschweren würde. Eine feste Integration in die Lehrpläne bereits in den ersten Jahren weiterführender Schulen scheint unumgänglich, um Kindern Medienkompetenz – zu der heute selbstverständlich auch eine Datenschutzkompetenz gehören muss – zu vermitteln und damit Selbstdatenschutz aufzubauen. Ergänzend dazu wäre ein Bildungsangebot auf digitalem Weg denkbar, wobei Kinder spielend an das komplexe Thema herangeführt und gut ausgebildet werden, um sich selbst schützen zu können, wo rechtliche Rahmen nicht ausreichend Schutz bieten können. Ein Beispiel wäre ein Serious Game, das es Kindern ermöglicht Erfahrungen zu sammeln, ohne dass bereits echte Konsequenzen entstehen, ihnen aber aufzeigt, was passiert, wenn sie leichtfertig oder unnötig Daten teilen, ohne auf die eigene Privatsphäre zu achten.

Literaturverzeichnis

Berman, G./Albright, K. (2017). Children and the Data Cycle: Rights and Ethics in a Big Data World. Innocenti Working Paper 2017-05, UNICEF Office of Research, Florence.

Brief, N./Raguse, M. (2015). Virtuelles Datenschutzbüro: Datenschutz bei Kindern. In: Virtuelles Datenschutzbüro v. 21. Oktober 2015. URL: https://www.datenschutz.de/datenschutz-bei-kindern/

Däubler W./Wedde, P./Weichert, T./Sommer, I. (2018): EU-Datenschutz-Grundverordnung und BDSG-neu: Kompaktkommentar. Frankfurt am Main: Bund-Verlag.

Europäischer Datenschutzausschuss (2017). Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt". WP 248 Rev. 01.

Europäischer Datenschutzausschuss (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251rev.01.

GPEN (2016). Global Privacy Enforcement Network: Annual Report 2015. URL: https://www.privacyenforcement.net/sites/default/files/Annual%20Report%20Final%20Version.pdf

Hagendorff, T. (2017). Das Ende der Informationskontrolle: Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz. Bielefeld: transcript Verlag.

Heesen, J. (Hrsg., 2016). Handbuch Medien- und Informationsethik. Stuttgart: J.B. Metzler.

Herschel, R./Miori, V.M. (2017). Ethics & Big Data. In: Technology in Society 49 (2017), S. 31-36.

Kommission für Jugendmedienschutz. Abgerufen am 10.01.2018 von http://www.kjm-online.de/fileadmin/Download_KJM/Recht/JMStV_ge%C3%A4nd._durch_19._R%C3%84StV.pdf

Livingstone, S./Third, A. (2017). Children and young people's rights in the digital age: an emerging agenda. In: New Media & Society. 19 (5), S. 657-670.

Livingstone, S./Yoo D.Y. (2017). More clarity brings more confusion: debating

what the European General Data Protection Regulation means for children in the UK. In: LSE Media Policy Project Blog, 18.1.2018, URL: https://www.childinthecity.org/2018/02/14/what-the-european-general-data-protection-regulation-means-for-children-in-the-uk/

Maier, S. (2017). DSGVO: Informationspflicht & Interessenabwägung bei Daten von Kindern. In: Datenschutzbeauftragter.info, v. 1.8.2017 (URL: https://www.datenschutzbeauftragter-info.de/dsgvo-informationspflicht-interessenabwaegung-bei-daten-von-kindern/).

Medienpädagogischer Forschungsverband Südwest (Hrsg., 2016). KIM-Studie 2016: Kindheit, Internet, Medien – Basisstudie zum Medienumgang 6- bis 13-Jähriger in Deutschland. Stuttgart.

Mönkeberg, S. (2015). Bilder und Reflexionen vom Ich: Das Web 2.0 als Institution der Selbstthematisierung? In Grimm, P., Keber, T. & Zöllner, O. (Hrsg.). Anonymität und Transparenz in der digitalen Gesellschaft. Stuttgart: Franz Steiner Verlag.

Nebel, M. (2015). Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken. In Richter, P. (Hrsg.). Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data. Baden-Baden: Nomos Verlagsgesellschaft.

Nohr, H. (2017). Big Data im Lichte der EU-Datenschutz-Grundverordnung. In: JurPC Web-Dok. 111/2017, Abs. 1-86 (http://www.jurpc.de/jurpc/show?id=20170111).

o.V. (2018). Neue Altersgrenze: WhatsApp erst ab 16 Jahren erlaubt. In: Schau hin v. 25.04.2018, URL: https://www.schau-hin.info/news/artikel/neue-altersgrenze-whatsapp-erst-ab-16-jahren-erlaubt.html

o.V. (2012). Schutz der Daten von Kindern und Jugendlichen. In: Informationen für Erziehungsberatungsstellen 1/12, S. 14-17.

Tabatabai, E./Kim, A. (2016). Kids, Cookies And COPPA: Firms Pay A Price On Privacy. In: Law360, September 30, 2016. URL: https://www.law360.com/articles/845350/kids-cookies-and-coppa-firms-pay-a-price-on-privacy.

Topelson, D./Bavitz, C./Gupta, R./Oberman, I. (2013). Privacy and Children's Data - An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. The Berkman Center for Internet & Society at Harvard University. URL: https://cyber.harvard.edu/publications/2013/privacy_and_childrens_data.

Viola de Azevedo Cunha, M. (2017). Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy. Innocenti Working Paper 2017-03, UNICEF Office of Research, Florence.

Weichert, T. (2016): Die Europäische Datenschutz-Grundverordnung – Ein Überblick. In: Datenschutz Nachrichten 39 (2016) 2, S. 48-56.

Fußnoten

1 Kathrin Häring (BSc) bearbeitet im Master of Media Research an der Hochschule der Medien in Stuttgart das Projekt „Datenschutzbewusstsein bei der Social-Media-Nutzung von Kindern und Jugendlichen". Prof. Holger Nohr lehrt und forscht im Master of Media Research an der Hochschule der Medien Stuttgart, insbes. zu den Themen Datenschutz / Privacy und Netzpolitik.

2 Vgl. Berman/Albright 2017, S. 12.

3 Diese Ergebnisse aus dem laufenden Projekt „Datenschutzbewusstsein bei der Social-Media-Nutzung von Kindern und Jugendlichen" wurden auf der Jahrestagung 2018 der Fachgruppe Kommunikations- und Medienethik der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft vorgestellt.

4 Vgl. Hagendorff 2017, S. 7.

5 Vgl. Medienpädagogischer Forschungsverband Südwest 2016.

6 Mönkeberg 2015, S. 97.

7 Vgl. Berman/Albright 2017, S. 12.

8 Vgl. Berman/Albright 2017, S. 3.

9 Vgl. Berman/Albright 2017; Herschel/Miori 2017.

10 Vgl. Livingstone/Third 2017, S. 13.

11 Vgl. Livingstone/Third 2017, S. 6.

12 Vgl. GPEN, 2016 S. 11.

13 Vgl. Maier 2017.

14 Vgl. Däubler/Wedde/Weichert/Sommer 2018, S. 183.

15 Für eine Übersicht vgl. Topelson/Bavitz/Gupta/Oberman 2013 sowie Tabatabai/Kim 2016 zum Tracking und zu diesbezüglichen Bußgeldverfahren.

16 BGH, I ZR 218/12 (Url: https://openjur.de/u/691632.html).

17 Vgl. o.V. 2012.

18 Vgl. o.V. 2018.

19 Vgl. Weichert 2016.

20 Vgl. Däubler/Wedde/Weichert/Sommer 2018, S. 186.

21 Vgl. Livingstone/Yoo 2018 mit einer Übersicht über die EU-weit unterschiedlichen Altersgrenzen.

22 Vgl. Maier 2017.

23 Vgl. Maier 2017.

24 Ausführlich dazu Nohr 2017.

25 Vgl. Europäischer Datenschutzausschuss, 2018.

26 Europäischer Datenschutzausschuss, 2017.

27 Nebel 2015, S. 97.

28 Heesen 2016, S. 192.

29 Vgl. Berman/Albright 2017, S. 12; Livingstone/Third 2017, S. 10.

30 Vgl. Viola de Azevedo Cunha 2017, S. 12.

31 Vgl. Däubler/Wedde/Weichert/Sommer 2017, S. 184.

32 Vgl. Brief/Raguse 2015.

Presserklärung der Deutschen Vereinigung für Datenschutz e. V. vom 30.10.2018

NGOs fordern EU-Rat zum Beschluss über qualifizierte ePrivacy-Verordnung auf

Der Spiegel titelt derzeit „Das Internet ist kaputt". Die Einsicht, dass grundrechtswidrige Geschäftsmodelle und unkontrollierte Falschnachrichten im weltweiten Netz unsere Freiheiten und unsere Demokratie schädigen, ist nicht mehr nur eine Erkenntnis europäischer Bürgerrechtsorganisationen, sondern wird immer mehr selbst im Silicon Valley anerkannt. Regulierung ist gefordert. Europa hat hierzu mit der Datenschutz-Grundverordnung einen ersten Schritt gemacht. Nach Ansicht von vielen europäischen und 16 deutschen Nichtregierungsorganisationen (NGOs) – Bürgerrechts-, Verbraucherschutz- und Berufsverbänden – muss der nächste Schritt die schnelle Verabschiedung der ePrivacy-Verordnung in Europa sein. Schon seit zwei Jahren liegen hierzu die Vorschläge der EU-Kommission vor. Seit einem Jahr sind Verbesserungsvorschläge des EU-Parlaments bekannt. Doch der EU-Rat, in dem die deutsche Bundesregierung vertreten ist, blockiert die weitere Verabschiedung.

In einem offenen Brief, der an Wirtschaftsminister Peter Altmaier, Justiz- und Verbraucherschutzministerin Katarina Barley und Innenminister Horst Seehofer gerichtet ist, fordern nun die 16 NGOs von der Bundesregierung, die qualifizierte Regulierung des Datenschutzes im Bereich der Telekommunikation voranzutreiben und damit sowohl den dominanten US-Unternehmen wie auch der europäischen Internet-Lobby klarzumachen, dass im Internet freiheitliche und demokratische Werte gelten müssen, indem das ungebremste Datensammeln über Netznutzung und die Massenüberwachung verhindert werden und der rechtliche Schutz der elektronischen Kommunikation gesichert wird.

Frank Spaeing, Vorsitzender der Deutschen Vereinigung für datenschutz Datenschutz e. V. (DVD): „Der aktuelle Vorsitz des EU-Rats, Österreich, zeigt keine Neigung, den Internet-Regulierungsprozess voranzutreiben. Auch die Bundesregierung bremste bisher nach heftigem Wirtschaftslobbyismus insbesondere aus der IT-Wirtschaft den dringend nötigen Regulierungsprozess. Das muss sich ändern. Wir brauchen endlich moderne technikkonforme Regeln für den Bereich der Telekommunikation."

Werner Hülsmann, stellvertretender DVD-Vorsitzender: „Technischer Fortschritt darf nicht zulasten der Bürgerrechte stattfinden. Derzeit profitieren von der unterregulierten elektronischen Kommunikation insbesondere die US-Firmen Google und Facebook. Chinesische Firmen drängen auf den europäischen Markt. Eine schnelle qualifizierte Verabschiedung der ePrivacy-Verordnung und deren strenge Durchsetzung auf dem europäischen Markt ist der beste Schutz der einheimischen IT-Wirtschaft vor einer bisher ungebändigten US-amerikanischen und chinesischen Konkurrenz."

Der offene Brief wird neben der Deutschen Vereinigung für Datenschutz (DVD) u. a. unterstützt vom Arbeitskreis Vorratsdatenspeicherung, dem Bund demokratischer Wissenschaftlerinnen und Wissenschaftler, digitalcourage und dem Verbraucherzentrale Bundesverband.

Den Offenen Brief zum Schutz der elektronischen Kommunikation finden Sie unter https://dvd-ev.de/Brief-ePriv oder https://www.datenschutzverein.de/wp-content/uploads/2018/10/ePrivacy-Appell-Altmeier.pdf.

Presserklärung des Gerichtshofs der Europäischen Union (EuGH)

Vorabentscheidungssachen zu natürlichen Personen werden künftig anonymisiert

Nachdem die neue Datenschutz-Grundverordnung (DSGVO) seit kurzem gilt und demnächst die Datenschutzverordnung für die Organe der Europäischen Union in Kraft treten wird, hat der Gerichtshof beschlossen, den Schutz der Daten natürlicher Personen bei Veröffentlichungen zu Vorabentscheidungssachen zu verbessern.

Damit folgt er einer innerhalb der Mitgliedstaaten beobachteten Tendenz zur Verbesserung des Schutzes personenbezogener Daten im Kontext immer vielfältigerer Such- und Verbreitungsinstrumente. In der jüngeren Rechtsprechung des Gerichtshofs zeigt sich diese Tendenz im Übrigen in einer wachsenden Anzahl von Urteilen auf diesem Gebiet, die zu Fragen wie dem Recht auf Entfernung von Links aus Ergebnislisten in Suchmaschinen, der Gültigkeit der Entscheidung der Kommission, in der festgestellt wurde, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten würden, der Gültigkeit des Abkommens

über die Übermittlung und Verarbeitung von Fluggastdatensätzen (Passenger Name Record data – PNR) zwischen der Europäischen Union und Kanada, der Verantwortlichkeit der Betreiber von Facebook-Fanpages oder auch der Rechtmäßigkeit der Speicherung personenbezogener Daten durch Betreiber von elektronischen Kommunikationsdiensten ergangen sind.

Damit sowohl der Schutz der Daten von an Vorabentscheidungssachen beteiligten natürlichen Personen als auch die Information der Bürger und die Öffentlichkeit der Justiz gewährleistet werden, hat der Gerichtshof daher für alle ab 1. Juli 2018 anhängig gemachten Vorabentscheidungssachen entschieden, in allen seinen veröffentlichten Dokumenten den Namen der an der Rechtssache beteiligten natürlichen Personen durch Anfangsbuchstaben zu ersetzen. Ebenso werden alle ergänzenden Details, anhand deren die Betroffenen identifiziert werden können, weggelassen.

Diese neuen Leitlinien werden für alle Veröffentlichungen im Rahmen der Bearbeitung der Rechtssache von ihrer Einreichung bis zu ihrem Abschluss (Mitteilungen im Amtsblatt, Schlussanträge, Urteile ...) sowie für die Rechtssachenbezeichnung gelten. Sie betreffen nicht juristische Personen, denen der Gerichtshof auf ausdrücklichen Antrag einer Partei oder sofern die besonderen Umstände der Rechtssache es rechtfertigen, die Möglichkeit einer Ausnahme vorbehält.

Um die Zitierung und die Identifizierung der anonymisierten Rechtssachen zu erleichtern, wird jeder Rechtssache durch den Gerichtshof eine übliche Bezeichnung nach den folgenden Modalitäten zugeteilt:

- Wird die Rechtssache ausschließlich zwischen natürlichen Personen geführt, so wird die Rechtssachenbezeichnung aus zwei Anfangsbuchstaben bestehen, die für den Vor- und Nachnamen der Klägerpartei stehen, jedoch nicht mit dem tatsächlichen Vor- und Nachnamen dieser Partei übereinstimmen. Zur Verhinderung der Häufung von Rechtssachen mit den gleichen Anfangsbuchstaben (und da die Zahl der möglichen Buchstabenkombinationen nicht unbegrenzt ist) wird der Gerichtshof diesen beiden Anfangsbuchstaben in Klammern ein Unterscheidungsmerkmal hinzufügen. Dieses zusätzliche Element kann sich auf den Namen einer juristischen Person, die, ohne im Rechtsstreit Partei zu sein, genannt wird oder von der Rechtssache betroffen ist, oder auch auf den Gegenstand oder die Problematik des Rechtsstreits beziehen. Diese letztere Methode wurde beispielsweise im jüngsten Urteil des Gerichtshofs vom 26. Juni 2018 in der Rechtssache C-451/16, MB (Geschlechtsumwandlung und Ruhestandsrente), angewandt.
- Zählen in der Rechtssache natürliche und juristische Personen zu den Parteien, so wird die Rechtssache den Namen einer der juristischen Personen als Bezeichnung führen. Handelt es sich jedoch um eine Behörde, die regelmäßig Parteistellung vor dem Gerichtshof hat (z. B. Finanzminister), wird der Rechtssachenbezeichnung ebenfalls ein Unterscheidungsmerkmal beigefügt werden.

Zuletzt ist noch darauf hinzuweisen, dass die oben dargestellten Maßnahmen einen angemessenen Schutz personenbezogener Daten im Rahmen der Veröffentlichungen des Gerichtshofs gewährleisten sollen. Sie betreffen weder die Art und Weise der Bearbeitung der Rechtssachen durch den Gerichtshof noch den üblichen Verfahrensablauf und insbesondere nicht die mündlichen Verhandlungen, die weiterhin nach den derzeitigen Modalitäten ablaufen werden (EuGH PM Nr. 96/18 v. 29.06.2018).

Veröffentlichung gemäß Bayerischem Ministerratsbeschluss vom 5. Juni 2018

Datenschutz-Grundverordnung (DSGVO): Der Bayerische Weg zu einer bürgernahen und mittelstandsfreundlichen Anwendung

Der Ministerrat beschließt nachfolgenden Bayerischen Weg zu einer bürgernahen und mittelstandsfreundlichen Anwendung des Datenschutzrechts, die die Ziele der Datenschutz-Grundverordnung sachgerecht und mit Augenmaß verfolgt und damit auch ihre Akzeptanz in der Bevölkerung fördert:

– Kein Amateursportverein, keine Musikkapelle oder sonstige vor allem durch ehrenamtliches Engagement getragene Vereine müssen einen Datenschutzbeauftragten bestellen.
– Bei einem Erstverstoß im Dickicht der Datenschutzregeln drohen keine Bußgelder; Hinweise und Beratung haben Vorrang vor Sanktionen.
– Wir werden eine Praxis von Abmahnanwälten, die glauben bei Unternehmen formelle Datenschutzverstöße rechtsmissbräuchlich abmahnen und abkassieren zu können, nicht hinnehmen.
– Wir werden mit den Betroffenen weitere Bestimmungen im Datenschutzrecht identifizieren, bei deren Anwendung im Besonderen darauf hinzuwirken ist, dass die Ziele der Datenschutz-Grundverordnung sachgerecht und mit Augenmaß verfolgt werden.
– Hierzu werden wir weitere Gespräche mit Vereinen und Mittelständlern anbieten.

Quelle: Allgemeines Ministerialblatt der bayerischen Staatsregierung Nr. 9 v. 31.07.2018, S. 451

Bayerisches Landesamt für Datenschutzaufsicht

Klingelschild und Datenschutz

Nachdem nun nicht mehr nur eine Wiener Wohnungsbaugesellschaft ihre unsinnigen Pläne veröffentlicht hat, wegen der Datenschutz-Grundverordnung (DS-GVO) Klingelschilder bei Wohnblocks zu entfernen, sondern es auch in Deutschland derartige Bestrebungen gibt, ist es notwendig, klar und deutlich darauf hinzuweisen, dass es eine derartige Notwendigkeit aus datenschutzrechtlichen Gründen nicht gibt.

Die Namen auf Klingelschildern sind personenbezogene Daten. Die Datenschutz-Grundverordnung gilt für die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen". Das Anbringen von Klingelschildern ist keine automatisierte Verarbeitung. Selbst wenn man zu der kaum vertretbaren Auffassung gelangen sollte, dass gedruckte Namensschilder der Bewohner aus einer automatisierten Verarbeitung entstanden sind und die Anordnung der Klingelschilder im Eingangsbereich in einem Dateisystem erfolgt, weil sie die Lage der Wohnung wiedergibt und es damit zu einer Anwendung der Datenschutzgrundverordnung käme, wäre die Verarbeitung durch die Wohnungsbaugesellschaft in aller Regel nach Art. 6 Abs. 1 f DS-GVO datenschutzrechtlich zulässig.

In Einzelfällen mag es gerechtfertigt sein, dass der (richtige) Name von Bewohnern nicht auf dem Klingelschild steht. Bei gefährdeten prominenten Personen, Personen in einem Zeugenschutzprogramm oder bei Personen, die durch Stalking bedroht werden, mag eine pseudonymisierte Bezeichnung auf dem Klingelschild gerechtfertigt sein. Eine datenschutzrechtliche Notwendigkeit, alle Klingelschilder zu pseudonymisieren, das heißt den Namen durch eine andere Kennzeichnung wie Ziffern oder Buchstabenkombinationen zu ersetzen, gibt es nicht.

Zivilrechtlich, d.h. durch Hausordnungen oder sonstigen Vertrag kann das Ob und Wie (z.B. einheitliches Erscheinungsbild) der Klingelschilder geregelt werden. Dabei kann dann auch berücksichtigt werden, ob man wirklich Postdienstleistern, Rettungsdiensten und sonstigen Besuchern das Auffinden von Bewohnern erschweren möchte.

„Ich finde es sehr problematisch und auch sehr schade, dass durch diese unsinnigen Behauptungen die sehr gute Datenschutz-Grundverordnung als Begründung für etwas herangezogen wird, was sie gar nicht fordert und sie damit als „weltfremdes europäisches Recht" diskreditiert wird. Äußerungen in der Art, dass ein Mieter sich nur bei der Aufsichtsbehörde beschweren müsse, wenn sein Klingelschild nicht entfernt werde und die Aufsichtsbehörde dann ein Bußgeld von 20 Mio. EUR verhängen werde, was rechtlich völlig ausgeschlossen ist, zeigt, dass es hier um Panikmache oder Streben nach Medienpräsenz geht, aber jedenfalls nicht um wirklichen Datenschutz," so Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht.

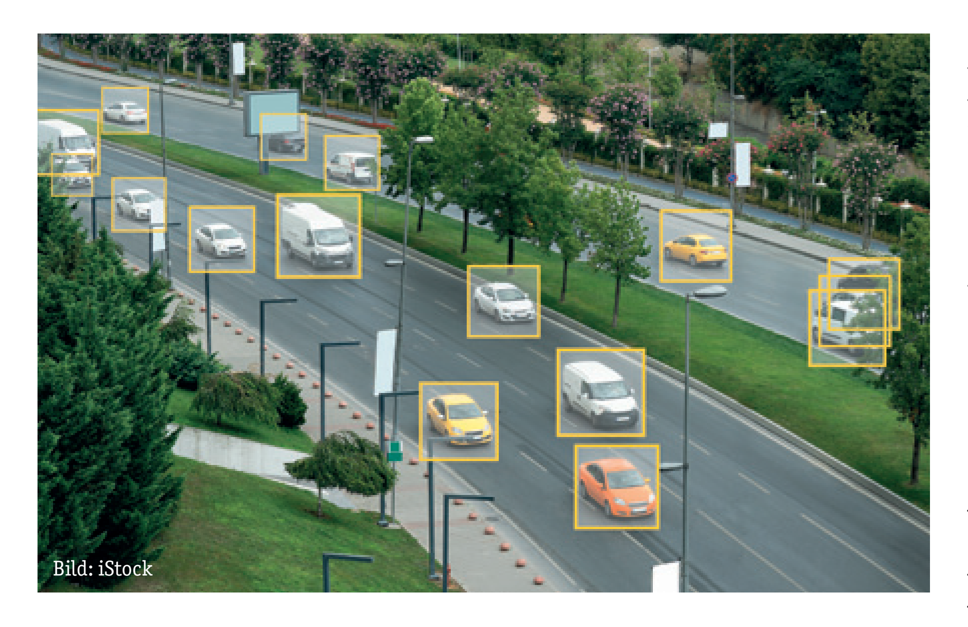
Thomas Kranig Präsident

Deutsche Vereinigung für Datenschutz e. V. (DVD)

Datenschützer: Geplante Kontrolle der Dieselverfahrverbote ist verfassungswidrig"

Die Vorschläge des Bundesverkehrsministeriums zur Überwachung von Dieselfahrverboten sind nach Einschätzung der Deutschen Vereinigung für Datenschutz e. v. (DVD) eindeutig verfassungswidrig: Sie sehen vor, dass nicht nur Kfz, die gegen ein Fahrverbot verstoßen, per Kfz-Kennzeichen-Scanning und mit einem Fahrerbild automatisiert erfasst werden, sondern sämtliche Kfz und deren Fahrzeugführer, die in eine Fahrverbotszone einfahren.

Frank Spaeing, DVD-Vorsitzender: „Diese Totalerfassung ist unverhältnismäßig. Daran ändert sich auch nichts dadurch, dass die Daten der Kfz, für die keine Fahrverbotsmerkmale im Kraftfahrtbundesamt (KBA) gespeichert sind, nach einer geplanten Datenübermittlung dorthin und einem Datenabgleich wieder gelöscht werden sollen. Die bisher vorgesehene Regelung des Ministeriums ist zudem wegen ihrer Unbestimmtheit verfassungswidrig. Aus ihr ergibt sich nicht im Ansatz, welche Datenverarbeitung tatsächlich durchgeführt werden soll. Im Fall einer Normenkontrolle würde das Bundesverfassungsgericht die geplante Regelung aufheben."


Bild: iStock

Werner Hülsmann, stellvertretender DVD-Vorsitzender, ergänzt: „Es gäbe datensparsamere technische Alternativen, etwa das Anbringen von RFID-Chips an fahrbeschränkte Dieselfahrzeuge, über die eine ausschließliche Erfassung solcher Kfz erreicht werden könnte. Datensparsamer wären natürlich auch die diskutierten blauen Plaketten, die von Polizeibeamten oder Ordnungsbehörden kontrolliert werden müssten. Das zentrale Problem liegt aber unseres Erachtens nach ganz woanders: Die Fahrverbote werden von den Gerichten nur verhängt, weil die Politik die Kfz-Hersteller nicht zur Nachrüstung schmutziger Dieselfahrzeuge verpflichtet. Würde diese Nachrüstung politisch durchgesetzt, dann würde nicht nur die Umwelt effektiver geschützt, es müssten auch überhaupt keine Kontrollen durchgeführt und Daten erfasst werden. Hier wird, um die Kfz-Hersteller zu schonen, ein Überwachungsnetz über die Kfz-Nutzenden ausgeworfen."

Der offene Brief wird neben der Deutschen Vereinigung für Datenschutz (DVD) u. a. unterstützt vom Arbeitskreis Vorratsdatenspeicherung, dem Bund demokratischer Wissenschaftlerinnen und Wissenschaftler, digitalcourage und dem Verbraucherzentrale Bundesverband.

Den Offenen Brief zum Schutz der elektronischen Kommunikation finden Sie unter https://www.datenschutzverein.de/wp-content/uploads/2018/11/2018-11-DVD-PM-Dieselfahrverbote.pdf

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
November 2018

Der Datenschutzbeauftragte: Wettbewerbsvorteil für deutsche Unternehmen und Schutz von Verbraucherrechten

Positionspapier zur Benennungspflicht eines betrieblichen Datenschutzbeauftragten in kleinen und mittelständischen Unternehmen

Im Zuge der digitalen Transformation von Wirtschaft und Gesellschaft hat die Erfassung und Verarbeitung von personenbezogenen Daten rasant an Bedeutung gewonnen. Die Bundesregierung unterstreicht regelmäßig den herausragenden Stellenwert von Daten für die deutsche Wirtschaft. Sie sind mittlerweile zentraler Wettbewerbs- und Wachstumsfaktor für viele Unternehmen – nicht nur für Konzerne, sondern gerade auch für KMU. Vor dem Hintergrund fällt dem betrieblichen Datenschutzbeauftragten eine Schlüsselrolle bei der Gewährleistung der rechtssicheren Datenverarbeitung der Unternehmen und dem Schutz der Grundrechte der betroffenen Personen, also der Bürger und Beschäftigten, zu.

Datenschutzbeauftragte sorgen für sichere Umsetzung komplexer Vorschriften

Durch die Europäische Datenschutz-Grundverordnung (DS-GVO) sind Unternehmen zur Einhaltung einer Reihe von komplexen und umfangreichen gesetzlichen Vorgaben verpflichtet – und dies ganz unabhängig davon, ob die gesetzlichen Bestimmungen die Benennung eines Datenschutzbeauftragten vorschreiben.

Die Gewährleistung der datenschutzrechtlichen Vorgaben ist ein „moving target", da sich die Anforderungen durch Auslegungen, Rechtsprechung und ergänzende Richtlinien weiterentwickeln und verändern. Ohne die Unterstützung des betrieblichen Datenschutzbeauftragten sind die meisten datenschutzrechtlichen Vorgaben für kleine und mittelständische Unternehmen ein „invisible tar-

get“. Sie erhalten kaum einen Zugang zu diesen Vorgaben und können somit die Einhaltung der datenschutzrechtlichen Anforderungen kaum gewährleisten. Der Datenschutzbeauftragte berät Unternehmen, kontrolliert und überwacht die Umsetzung, so dass sie die datenschutzrechtlichen Anforderungen zuverlässig erfüllen können. Mit seinem Fachwissen schafft er Transparenz über die zu berücksichtigenden Regelungen und begleitet die Anwendung der rechtlichen Vorschriften. Er analysiert das Datenschutzniveau des Unternehmens, berät bei Umsetzungsmaßnahmen, konzipiert notwendige Unternehmensrichtlinien, begleitet die erforderlichen Prozesse, schult Mitarbeiter im Datenschutz und unterstützt bei der Einhaltung der gesetzlichen Rahmenbedingungen.

Der Datenschutzbeauftragte hat aber nicht nur die Bedürfnisse und Entwicklungen der Unternehmen im Blick, sondern stellt zudem sicher, dass das Grundrecht auf informationelle Selbstbestimmung, das Recht auf Datenschutz, gewährleistet wird. Mit seinem Know-how und seiner Erfahrung unterstützt er wirksame und praktikable Lösungen für den Datenschutz, die sowohl im Sinne der Wirtschaft als auch der Betroffenen sind. Für die Bürger und die Beschäftigten, deren personenbezogene Daten verarbeitet werden, stellt er somit zugleich den Qualitätsbeleg einer datenschutzkonformen Verarbeitung dar. Dieser Beleg kann durch das Unternehmen auch zur Positionierung und Abgrenzung vom Wettbewerb im In- und Ausland herangezogen werden.

Die gesetzliche Benennungspflicht dient somit insbesondere dem Schutz der Bürger und Beschäftigten, die auf den Schutz ihrer persönlichen Daten im Rahmen von Datenverarbeitungsprozessen in Unternehmen und Behörden vertrauen können.

Handlungsempfehlungen: Modell des betrieblichen Datenschutzbeauftragten als Wettbewerbsvorteil erhalten und zukunftsorientiert ausgestalten

Der Datenschutzbeauftragte ist eine langjährige Erfolgsgeschichte des deutschen Datenschutzrechts. Er hat eine erhebliche entlastende Wirkung für die Unternehmen und sichert die Rechte der Bürger. Zur Fortschreibung dieser Erfolgsgeschichte schlagen wir folgende Maßnahmen vor:

1 Die Funktion des betrieblichen und behördlichen Datenschutzbeauftragten bleibt durch die Benennungspflicht auf nationaler Ebene verankert, um die Umsetzung der datenschutzrechtlichen Anforderungen zu ermöglichen und die Rechte der Bürger in Zusammenhang mit der Verarbeitung ihrer Daten zu gewährleisten.

2 Datenschutz muss viel stärker als bisher als Wettbewerbs- und Standortvorteil begriffen werden. Um diesen für die deutsche Wirtschaft erfolgreich zu nutzen und zu erhalten, müssen Datenschutzbeauftragte auch weiterhin intensiv in die Prozesse der Datenverarbeitung eingebunden werden.

3 Bürokratische Hürden müssen abgebaut werden, um die Umsetzung des Datenschutzrechts, insbesondere für den Mittelstand sowie Vereine und Institutionen, zu vereinfachen. Durch eine praxistaugliche Ausgestaltung von Dokumentationsanforderungen und die stärkere Einbeziehung des Datenschutzbeauftragten bei diesen Tätigkeiten können deutliche Erleichterungen geschaffen werden und effektiver Kosten gesenkt bzw. vermieden werden als dies mit einer Abschaffung der Benennungspflicht des Datenschutzbeauftragten möglich wäre.

Mit der Umsetzung dieser Handlungsempfehlungen werden kleine Organisationen und mittelständische Unternehmen spürbar entlastet.



Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. vertritt die Belange von rund 1.600 betrieblichen und behördlichen Datenschutzbeauftragten und Beratern aus ganz Deutschland. 1989 gegründet, ist er die älteste Interessenvertretung der Branche.

Prof. Dr. Alexander Roßnagel
Leiter des Fachgebiets und Professor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes am Fachbereich Wirtschaftswissenschaften der Universität Kassel.

Prof. Dr. Jürgen Taeger
Universitätsprofessor an der Carl von Ossietzky Universität Oldenburg und bekleidet den Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Rechtsinformatik.

ADM.

Der ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. vertritt die Interessen der privatwirtschaftlichen Markt- und Sozialforschungsinstitute in Deutschland. Er wurde im Jahr 1955 gegründet und ist der einzige Wirtschaftsverband dieser Art. Gegenwärtig gehören ihm 73 privatwirtschaftliche Forschungsinstitute an, die zusammen rund 83 Prozent des Umsatzes der deutschen Markt-, Meinungs- und Sozialforschung erzielen (2017: 2,45 Mrd. €). Zu den satzungsgemäßen Aufgaben des ADM gehören die Wahrung und Förderung der Wissenschaftlichkeit der Markt- und Sozialforschung, die Gewährleistung der Anonymität der Teilnehmer wissenschaftlicher Untersuchungen und die Entwicklung von Berufsgrundsätzen und Standesregeln.



Die DVD ist eine unabhängige Bürgerrechtsvereinigung, die sich für Datenschutzbelange in Deutschland und Europa einsetzt.



Die GDD tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen – insbesondere auch die Datenschutzbeauftragten – bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit

verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.



Die Stiftung Datenschutz wurde 2013 von der Bundesrepublik Deutschland gegründet. Aufgabe der unabhängigen Einrichtung ist die Förderung des Privatsphärenschutzes. Hierzu bietet sie eine Plattform zur Diskussion und dient als Schnittstelle zwischen Gesellschaft, Politik, Wirtschaft und Forschung.



Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. TeleTrusT ist Träger der „TeleTrusT European Bridge CA“ (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate „TeleTrusT Information Security Professional“ (T.I.S.P.) und „TeleTrusT Professional for Secure Software Engineering“ (T.P.S.S.E.) sowie des Vertrauenszeichens „IT Security made in Germany“. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

verbraucherzentrale
Bundesverband

Der Verbraucherzentrale Bundesverband ist die starke Stimme von mehr als 80 Millionen Verbrauchern in Deutschland. Der vzbv vertritt ihre Interessen gegenüber Politik, Wirtschaft und Verwaltung und klagt Verbraucherrechte vor Gericht ein. Als Dachverband der 16 Verbraucherzentralen der Länder und 25 Verbraucherschutzorganisationen bündelt er die Kräfte für einen starken Verbraucherschutz.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland


Bild: iStock

Bund

Kontrolle des Dieselfahrverbot als Vollüberwachung geplant

Die Überwachung der derzeit von Gerichten sukzessive für viele Städte angeordneten Diesel-Fahrverbote ist personalintensiv und teuer. In Hamburg zeigte sich z. B. bereits ein erhöhter Personalbedarf bei der Polizei zur Durchführung der Verkehrskontrollen. Daher plant die Bundesregierung eine automatisierte Erfassung aller VerkehrsteilnehmerInnen. In einem Gesetzentwurf, der klammheimlich am 07.11.2018 im Kabinett verabschiedet worden ist, ist dafür ein automatisierter Datenbankabgleich mit dem Kraftfahrt-Bundesamt (KBA) vorgesehen. Zu dem „Entwurf eines Neunten Gesetzes zur Änderung des Straßenverkehrsgesetzes“ hatten sich zuvor Interessenverbände der Polizei und von Überwachungstechnik-Herstellern positiv geäußert. Den datenschutzrechtlichen Regelungen des Gesetzentwurfs stimmten im Rahmen der Ressortanhörung das Bundesjustizministerium, das Bundesinnenministerium sowie die Bundesbeauftragte für Datenschutz (BfDI) zu. Der Ball liegt jetzt im Bundestag.

Der Gesetzentwurf soll es den Behörden erlauben, „im Rahmen von Kontrollen bestimmte Daten, auch automatisiert, erheben, speichern und verwenden sowie auf die Daten des Zentralen Fahrzeugregisters zugreifen“ zu können. Beim KBA sind die Halter- und Fahrzeugdaten über zugelassene Fahrzeuge gespeichert. Um in einem automatisierten Datenabgleich feststellen zu können, ob für bestimmte Fahrzeuge eine Verkehrsbeschränkung gilt, sollen die Behörden vor Ort das Fahrzeugkennzeichen, die Fahrzeugmerkmale, das Bild des Fahrzeugs und der FahrerIn „automatisiert“ erfassen und abgleichen dürfen. Das Bild der FahrerIn ist dabei erforderlich, weil sie verkehrsrechtlich persönlich haftet und daher identifiziert werden muss.

Die Datenerhebung soll in der Regel offen für jeden erkennbar erfolgen. Die Daten müssen spätestens sechs Monate nach ihrer Erhebung gelöscht werden, es sei denn es kommt zu einem Treffer: Die Daten der nicht fahrberechtigten Fahrzeuge müssen nach der Übermittlung an die für die Ordnungswidrigkeiten zuständige Verwaltungsbehörde „unverzüglich“ gelöscht werden. Im Entwurf wird davon ausgegangen, dass zur Umsetzung „keine weiteren Kosten“ entstehen. Die Interessenverbände sehen das anders. Sowohl die Deutsche Polizeigewerkschaft, als auch der Bundesverband für Verkehrssicherheitstechnik plädieren für den Aufbau einer „intelligenten Videoüberwachung“. Diese könnte mit einer Vignette oder einer Nummernschilderfassung kombiniert werden. Im letzteren Fall wäre auch die im Gesetz vorgesehene Abfrage des Zentralen Fahrzeugregisters notwendig.

Der Jurist und Datenschutzexperte Malte Engeler erklärte, das vorgesehene Verfahren könne nur dann verhältnismäßig sein, wenn es tatsächlich keine milderen Mittel der Durchsetzung gibt: „Man könnte technisch aber vorsehen, dass statt auf das optisch erfasste Kennzeichen auf andere speziell für diese Zwecke geschaffene Identifier zurückgegriffen wird, wie zum Beispiel kleine RFID-Funksender, wie sie etwa beim Mautsystem E-ZPass in den USA genutzt werden. Das wäre genauso geeignet und weniger invasiv.“ Er wies darauf hin, dass das geplante System nur dann funktioniert, wenn alle vom Dieselverbot betroffenen Fahrzeuge von den Händlern oder dem TÜV an das Kraftfahrt-Bundesamt gemeldet werden. Diese Vorfrage sei aber gerichtlich umstritten. Letztlich werde damit „eine Überwachungsinfrastruktur auf Basis eines ‚harmlosen Anlasses‘ auf- und ausgebaut, die später mit wenigen Handgriffen zu hochproblematischen Zwecken genutzt werden kann.“

Rena Tangens vom Bürgerrechtsverein Digitalcourage erklärte: „Es ist unsäglich, dass die Politik die Autokonzerne nicht zu einer technischen Nachrüstlösung verpflichtet, dafür für symbolische Fahrverbote eine Überwachungsinfrastruktur für alle Leute aufbauen will, die in die Innenstadt fahren.“ Um die Automobilhersteller nicht zu brüskieren, werde das eigentliche Problem nicht angepackt: Statt den öffentlichen Personennahverkehr und eine Radinfrastruktur schnell auszubauen, werde in eine automatisierte Überwachung investiert, die von den Polizeiverbänden bereits seit Jahren für andere Zwecke gefordert wurde.

Konstantin von Notz, stellvertretender Vorsitzender der grünen Bundestagsfraktion, erklärte, es sei klar, dass die Einhaltung von Fahrverboten kontrolliert werden müsse. Doch der vorliegende Vorstoß der Bundesregierung schieße „weit über's Ziel hinaus“. Bundesverkehrsminister Andreas Scheuer wolle anlasslos alle Gebiete, für die Fahrverbote gelten, und alle einfahrenden Pkw dauerhaft überwachen. Es solle eine vollautomatisierte Überwachungsinfrastruktur installiert werden, die ausschließlich der zufälligen stichprobenartigen Kontrolle von möglichen Ordnungswidrigkeits-Verstößen diene. Das sei „absolut unverhältnismäßig und verfassungsrechtlich bedenklich“ (Schulzki-Haddouti, Bundesregierung plant offenbar Massenüberwachung bei Diesel-Fahrverboten, www.heise.de 15.11.2018).

Bund

Positivliste zur Datenschutz-Folgenabschätzung

Nachdem die Datenschutzaufsichtsbehörden einzelner Länder den Anfang gemacht hatten, hat nun auch die Datenschutzkonferenz (DSK) eine Positivliste zur Datenschutz-Folgenabschätzung (DSFA) herausgegeben. Diese ersetzt die bisherigen Listen für den nichtöffentlichen Bereich der einzelnen Aufsichtsbehörden und versteht sich als Anwendungshinweis für Unternehmen und Organisationen, die Verfahren anwenden, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Diese sind nach Art. 35 DSGVO verpflichtet, vorab eine Abschätzung der Folgen solcher vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

In der Liste sind insgesamt 17 Verarbeitungstätigkeiten aufgeführt, für die die DSK eine DSFA für erforderlich hält. Darunter befindet sich zum Beispiel die umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen, wie sie bei der Sammlung und Auswertung von Fahrzeugdaten der Fall ist. Auch die Erstellung umfassender Nutzerprofile in sozialen Netzwerken oder Dating-Portalen gehört dazu. Die Punkte finden sich weitgehend auch auf den bereits veröffentlichten DSFA-Positivlisten der einzelnen Länder. Die DSK ist der Zusammenschluss der unabhängigen Datenschutzbehörden des Bundes und der Länder. In ihren mindestens zweimal jährlich stattfindenden Tagungen stimmen sich die Mitglieder über aktuelle Themen ab (Kleijn, Datenschutzkonferenz veröffentlicht DSFA-Positivliste, www.heise.de 25.07.2018 mit Aktualisierungen der Redaktion; die aktuelle Version 1.1. vom 17.10.2018 der Liste findet sich unter https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf).

Bund

Microsoft ändert Cloud-Strategie

Microsoft will seine Cloud-Dienste von Azure über Office 365 bis hin zu Dynamics 365 künftig nur noch im Rahmen seines komplett in Eigenregie betriebenen Microsoft-Cloud-Netzwerks anbieten. Angesichts unvereinbarer Anforderungen der Gesetzeslagen in der EU und in den USA für international agierende Unternehmen hatte Microsoft im November 2015 das „Modell Microsoft Cloud Deutschland“ vorgestellt. Dabei werden die Rechenzentren für die betroffenen Dienste ausschließlich von der Deutschen Telekom als Datentreuhänder betrieben. Microsoft-Mitarbeitende hatten normalerweise keinen Zugang. Nur im Fall technischer Probleme, die sich ausschließlich durch Mithilfe von Microsoft ausräumen lassen, erhielten Mitarbeitende stundenweise unter besonderer Protokollierung Zugang zu den involvierten Rechenzentren. Microsoft konnte sich dann aber immer noch in der Pflicht sehen, den Forderungen amerikanischer Behörden auf Datenherausgabe zu folgen, wäre dazu aber aus technischen Gründen gar nicht in der Lage.

Seit der Einführung des Modells gab es vereinzelte Hinweise, dass das aufpreispflichtige Treuhänder-Angebot nur schwer mit anderweitigen internationalen Cloud-Angeboten kompatibel sei. In einem Blogbeitrag vom 31.08.2018 verkündete Microsoft nun, es werde die Cloud mit Datentreuhänderschaft ab jetzt nicht mehr für Neukunden anbieten. Für diese werden die Cloud-Dienste über europäische Rechenzentren und – sobald verfügbar – über neue Rechenzentren in Deutschland angeboten. Bestandskunden sollen voraussichtlich ab Ende 2018 Hilfen für die Migration auf alternative Rechenzentren erhalten. Bis dahin will Microsoft für die Cloud Deutschland keine neuen Dienste mehr bereitstellen.

Der Konzern versichert in seiner Trust-Center-Webseite, er werde die europäische Datenschutz-Grundverordnung (DSGVO) erfüllen und habe entsprechende Zusicherungen in seine Vertragsbestimmungen aufgenommen. Danach haben die KundInnen das Recht, persönliche Daten korrigieren, ergänzen oder löschen zu lassen, Datenlecks zu recherchieren und zu melden. Ein Statement, wie sich Microsoft im Fall eines Datenabflusses, z. B. an das Department of Homeland Security, verhalten wird, ist in der Veröffentlichung nicht zu finden.

Die Deutsche Telekom, die bisher nach eigener Auskunft mehr als ein Viertel ihrer Office365-Kunden zu den Bedingungen der Microsoft Cloud Deutschland bediente, will diesen Support so lange wie möglich aufrechterhalten und erklärte: „Im Ausblick auf die bevorstehenden Änderungen in der Microsoft-Strategie hat die Deutsche Telekom ein Service-Portfolio aufgebaut, das unseren Kunden die Möglichkeit gibt, auch weiterhin besonders sichere Cloud-Umgebungen zu nutzen“ (Schüler, Auslaufmodell: Microsoft Cloud Deutschland, www.heise.de 31.08.2018).

Bund

BAMF informiert BfV

Das Bundesamt für Migration und Flüchtlinge (BAMF) hat zwischen 2015 und 2017 in insgesamt 13.586 Fällen Informationen einschließlich personenbezogener Daten an das Bundesamt für Verfassungsschutz (BfV) übermittelt. Das geht aus der Antwort (BT-Drs. 19/3840) der Bundesregierung auf eine Kleine Anfrage (BT-Drs. 19/3573) der Fraktion Die Linke hervor. Die Zahl der Übermittlungen des BAMF an den Verfassungsschutz ist dabei in den drei Jahren sprunghaft gestiegen: Von 571 Fällen im Jahr 2015 auf 2.418 ein Jahr später und 10.597

im Jahr 2017 (Deutscher Bundestag, 27.08.2018 hib 618/2018).

Bund

BAMF-Sprachanalyse-Software unzuverlässig

Die Firma NUANCE hat für das Bundesamt für Migration und Flüchtlinge (BAMF) eine sogar preisgekrönte Software entwickelt, mit der die Herkunftsregion von Schutzsuchenden anhand der Sprache erkannt werden soll, allerdings nur für einige wenige Sprachen. Hierzu wird ein Schutzsuchender an ein Telefon gesetzt; er soll verschiedene Bilder interpretieren und das in seiner Heimatsprache mindestens 60 Sekunden, vorzugsweise 2 Minuten schildern. Danach kommt nach kurzer Zeit die Rückmeldung vom Computer.

Es wird u. a. über den Fall eines Mannes aus dem Norden Iraks berichtet, der Sorani-Kurdisch spricht. Die Sprache kennt der Sprachcomputer nicht, was aber den Anhörenden vom BAMF nicht beeindruckte. Das Ergebnis war: Zu 60% spreche der Mann türkisch und zu 20% hebräisch. Das Asylgesuch des Mannes wurde abgelehnt. Er befindet sich im Klageverfahren. Nach Ansicht des Bundeskriminalamtes (BKA) sind Spracherkennungen „von unter 75% völlig zu vernachlässigen“! (ANA-ZAR 4/2018, 71).

Bundesweit

Fahndung wegen Kindergeldbetrug

Von 2019 an wollen die Familienkassen in allen deutschen Großstädten nach Kindergeld-Betrug fahnden. Mithilfe spezieller Computerprogramme und in Kooperation mit dem Zoll, mit Schulämtern, den Einwohnermeldeämtern, Steuerbehörden und ausländischen Sozialämtern sollen Familien aufgespürt werden, die z. B. mit gefälschten ausländischen Geburtsurkunden oder Pässen staatliche Leistungen für nicht existierende Kinder kassieren. Karsten Bunk, Leiter der Familienkasse bei der Bundesagentur für Arbeit, erklärte, dass in Wuppertal und Düsseldorf bei der Kontrolle von 100 Verdachtsfällen kürzlich 40 ungerechtfertigte Anträge gefunden worden seien. Dadurch wurden rund 400.000 € Kindergeld zu Unrecht ausgezahlt. Zwar seien die Zahlen nicht repräsentativ, aber genug Anlass, die Kontrollen auf die gesamte Republik auszuweiten, beginnend in Hamburg und Bremen. In allen 14 regionalen Familienkassen Deutschlands sollen jeweils zwei Beschäftigte ausschließlich nach Missbrauchsfällen fahnden. Bunk forderte, die Datenschutzregeln für den Informationsaustausch zwischen den beteiligten Behörden zu lockern (Fahndung nach Betrügern, Der Spiegel Nr. 33 11.08.2018, 24).

Bundesweit

Fax-Betrüger ködern mit Datenschutz

Seit Oktober 2018 erhielten viele Unternehmen eine „eilige FAX-Mitteilung“ einer sog. „Datenschutzauskunft-Zentrale“, in der sie dazu gedrängt wurden, ein Formular auszufüllen, angeblich um der gesetzlichen Pflicht zur Umsetzung des Datenschutzes nachzukommen. Dazu stellte Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, klar: „Bei der „Datenschutzauskunft-Zentrale“ handelt es sich nicht um eine offizielle Stelle oder gar um eine Aufsichtsbehörde. In dem Fax werden die Unternehmen dazu gedrängt, ihre Firmen- und Betriebsdaten in einem Formular anzugeben und dieser „Datenschutzauskunft-Zentrale“ mitzuteilen. Es wird der falsche Eindruck erweckt, dies gewährleiste die Einhaltung der Datenschutzanforderungen. Der Haken steckt im Kleingedruckten: Mit Absenden des Formulars bestellt man kostenpflichtig Leistungen zum „Basisdatenschutz“ – jährlich werden dann 498,00 € fällig. Was mit „Basisdatenschutz“ gemeint sein soll, ist unklar. Eine Telefonnummer sucht man vergebens, die Webseite enthält kaum Informationen, und der Faxversender sitzt anscheinend in Malta und nicht – wie im Schreiben nahegelegt – in Deutschland. Seriös ist das nicht!“

Hansen appelliert an die Empfänger dieses Faxes, nicht voreilig das Formular auszufüllen und versehentlich einen Vertrag abzuschließen: „Es ist bedauerlich, wenn Datenschutz als Masche zur Abzocke missbraucht wird und versucht wird, die erfreulicherweise mittlerweile bei vielen vorhandene Sensibilisierung für das Thema Datenschutz derart auszunutzen. Ich empfehle, die vorhandenen Materialien auf den Webseiten der Datenschutzbehörden zu nutzen und – wenn nötig – Dienstleister für Rat und Tat zur Datenschutz-Compliance bewusst auszuwählen“ (PM ULD Schleswig-Holstein, Keine Abzocke mit Datenschutz – nicht auf das Fax der „Datenschutzauskunft-Zentrale“ hereinfallen, 02.10.2018).

Verschiedene Bundesländer

AfD-Schulmeldeportale fordern zur Denunzierung auf

Ende Oktober 2018 starteten die AfD-Bürgerschaftsfraktionen in Brandenburg und Berlin jeweils ein Meldeportal für SchülerInnen zur Denunzierung von AfD-kritischen Lehrkräften. Zuvor war ein solches Portal in Hamburg und in Baden-Württemberg ans Netz gegangen und hat Irritationen und Kritik ausgelöst.

Die AfD-Fraktion in der Hamburger Bürgerschaft erklärt in ihrer Datenschutzerklärung, „dass Minderjährige ihr ohne Mitwirkung ihrer Eltern keine personenbezogenen Daten übermitteln sollten und dass sie personenbezogene Daten Minderjähriger auch nicht sammelt“. Doch könne das elektronische Kontaktformular, mit dem „wirkliche oder vermeintliche Verstöße“ gegen das Neutralitätsgebot der Lehrkräfte gemeldet werden könnten, „natürlich auch von Minderjährigen ohne Mitwirkung der Eltern ausgefüllt und abgeschickt werden“. Aus der Darstellung ging nicht hervor, wann die Daten der meldenden Personen gelöscht werden. Hamburgs Schulsenator Ties Rabe nannte das Portal einen „albernen Mediengag“, der von seiner Lehrerschaft „wenig ernst genommen“ werde, meinte aber auch: „Hier sollen Lehrer eingeschüchtert und Schüler zu Denunzianten erzogen werden. Die AfD tut genau das, was sie anderen vorwirft: Sie politisiert die Schule und missbraucht Schüler für ihre politischen Ziele“. In der Vergangenheit sei seine Behörde „allen ernsthaften Hin-

weisen auf Verletzung der Neutralität nachgegangen. Bisher hat es allerdings kaum Fälle gegeben."

Vor der Inbetriebnahme in Berlin erklärte Beate Stoffers (SPD) von der dortigen Senatsverwaltung, dass es „per se nicht rechtswidrig" sei, „wenn eine private Organisation dazu auffordert (angebliche) staatliche Missstände zu melden". Allerdings könne „im Einzelfall" eine Meldung gegen Rechtsvorschriften verstoßen. Die Behörde halte es überdies für „überprüfungswürdig", ob die personenbezogenen Daten der gemeldeten Lehrkräfte wirklich nur an die zuständigen Behörden gemeldet werden. Sie meinte, es stehe „dem Schulfrieden entgegen", ein derartiges Portal auf den Weg zu bringen. Zuvor hatte schon ihre Brandenburger Parteifreundin, Bildungsministerin Britta Ernst, von einem „Angriff auf den Schulfrieden" gesprochen. Gerade in den ostdeutschen Bundesländern fühlten sich viele „zu Recht an Stasi-Überprüfungsmethoden erinnert".

In Brandenburg erklärte Parlamentspräsidentin Britta Stark (SPD), dass sie die Finanzierung des Portals prüfen lässt. Es bestehe der Verdacht auf Zweckentfremdung öffentlicher Mittel. Es bestünden erhebliche rechtliche Zweifel, ob Fraktionsmittel für das Portal ausgegeben werden dürfen. Nach einer Prüfung könnten die Gelder von der AfD-Fraktion zurückgefordert werden. Der Präsident des Berliner Abgeordnetenhauses, Ralf Wieland, zeigte sich zurückhaltender. Ein Sprecher sagte, nur der Landesrechnungshof könne die Verwendung von Fraktionsgeldern prüfen. Die Vorgänge würden beobachtet. Es könne durchaus sein, dass der Rechnungshof die Ausgaben der AfD-Fraktion mit Blick auf das Portal früher prüfen werde, als im langjährigen Turnus vorgesehen.

Bildungsministerin Ernst will untersuchen lassen, ob die gewählte Form der Plattform rechtlich erlaubt sei. Sie kündigte an, dass ihr Haus „wenn nötig Lehrkräfte unterstützen werde", auch durch Rechtsschutz. Im Hamburg habe die Zivilgesellschaft „kreativ gegen so eine Meldeplattform protestiert". AfD-KritikerInnen haben dort mit eigenen „Meldungen" die Plattform geflutet. Ein ähnliches Phänomen gab es in Baden-Württemberg, als der dortige AfD-Abgeordnete Stefan Räpple eine eigene Plattform starten wollte: Das Vorhaben hatte für besonderen Wirbel gesorgt, weil Räpple angekündigt hatte, auch die Namen von Lehrern veröffentlichen zu wollen. Schon nach einem Tag musste der – wegen seiner Nähe zu Wolfgang Gedeon selbst in der eigenen Fraktion zwischenzeitlich in Misskredit geratene – Abgeordnete seine Seite vorläufig vom Netz nehmen.

Was die Veröffentlichung von Lehrernamen anbelangt, klingt Räpple inzwischen vorsichtiger als zu Beginn der Aktion. Die Veröffentlichung sei nur die „Ultima ratio" und müsse noch geprüft werden. Er werde sich aber „nicht scheuen, es auf einen Rechtsstreit ankommen zu lassen". Letztlich sei das „eine juristische Frage". Es gebe jedenfalls ein „öffentliches Interesse", die Lehrernamen zu erfahren, da Schüler der Schulpflicht unterlägen und daher das Recht haben müssten zu wissen, wenn sie einen Lehrer hätten, der bereits durch Indoktrination aufgefallen sei. Bildungssenatorin Scheeres aus Berlin erinnerte daran, dass es „ausreichend Beschwerdeinstanzen" in den Schulen gebe. Die könnten genutzt werden, falls man meine, dass eine Lehrkraft sich nicht neutral verhalte.

In Baden-Württemberg hatte das Lehrer-Meldeportal nicht einmal einen Tag lang funktioniert. Bereits am Morgen nach der Freischaltung meldete der Abgeordnete Stefan Räpple auf der Internetseite „www.stefan-raepple.de/mein-lehrer-hetzt": „Leider kam es auf dieser Seite zu einem Hackerangriff." Die Seite werde „in Kürze wieder zur Verfügung" stehen, was aber nicht gelang. Die baden-württembergische Piratenpartei teilte mit, dass zehntausende Menschen ihr Angebot angenommen hätten, das Abgeordneten-Portal mit Hetz-Meldungen zu blockieren. Die „Piraten" sammelten unter „mein-abgeordneter-hetzt.de" Zitate von AfD-Abgeordneten, die sie als Hetze einstufen. Die Piratenpartei flutete damit nach eigenen Angaben das AfD-Lehrerportal. Michael Knödler, Vorsitzender der Piratenpartei Baden-Württemberg: „Unser Ziel war es, mit einer Aktion sowohl die menschenverachtenden Ideen der AfD aufzuzeigen als auch dem Denunziationsportal einige relevante Meldungen zukommen zu lassen." Spitzelei dürfe niemals Grundlage in einem demokratischen Rechtsstaat sein, und Listen von Personen seien datenschutzrechtlich bedenklich und deshalb kategorisch abzulehnen.

Gemäß Pressemeldungen haben nicht alle AfD-Fraktionen vor, solche Meldeportale zu starten: Nordrhein-Westfalen, Hessen und Schleswig-Holstein seien nicht dabei. Darüber hinaus gibt es Dispute über den richtigen Weg. So hält die AfD-Fraktion in Baden-Württemberg, anders als ihr Abgeordneter Räpple, nichts davon, die Namen von Lehrern in die Plattform aufzunehmen. AfD-Fraktionssprecher Klaus-Peter Kaschke erklärte, das könne „unter Umständen der Denunziation Tür und Tor öffnen". „Aus Erfahrung" wisse man zudem, dass Schüler-Aussagen „nicht immer stimmig" seien. Seine Fraktion wolle eine eigene Plattform „baldmöglichst" starten, aber erst nach „genauer Prüfung". Man müsse auch bedenken, dass so ein Vorhaben viele Kräfte binde.

Über das AfD-Meldeportal in Hamburg haben sich nach Angaben der Partei innerhalb kürzester Zeit 10.000 Menschen gemeldet. Der Hamburger Fraktionschef Alexander Wolf sagte, die Zuschriften ließen sich in drei Kategorien einteilen: Schüler und Eltern, die sich über AfD-feindliche Äußerungen von Lehrkräften beschwert hätten, Gegner der Partei sowie Menschen, die ihre Unterstützung für die Plattform zum Ausdruck bringen wollten. Wolf wehrte sich gegen den Begriff „Lehrer-Pranger". Es gehe nicht darum, die SchülerInnen zum Denunzieren zu erziehen. Als Beispiel für eine AfD-feindliche Aktion berichtete Wolf von einem Musiklehrer, der angeblich auf dem Klavier die Töne „A-F-D" gespielt und dies mit dem Satz „Das ist ja alles braune Soße." kommentiert haben soll.

Mitte Oktober 2018 wurde auf change.org eine Petition an die Kultusministerkonferenz gestartet, um „Solidarität mit Lehrkräften, die demokratische Werte und Vielfalt vermitteln" zum Ausdruck bringen. Motto: „Mein Lehrer fetzt". Nach entsprechenden Pressemeldungen hatten innerhalb von zwei Tagen bereits 30.000 Unterstützende die Online-Petition unterzeichnet („Alberner Medien-

gag", Der Spiegel Nr. 42 13.10.2018, 22; Vieth-Entus, Beschwerdeplattform in Berlin AfD-Meldeportal: Bildungssenatorin bangt um „Schulfrieden", www.tagesspiegel.de 18.10.2018; Piratenpartei entert Lehrer-Meldeportal der AfD, www.haz.de 13.10.2018).

Baden-Württemberg

CDU will Polizeirecht weiter verschärfen

Der Innenminister von Baden-Württemberg, Thomas Strobl (CDU), will trotz Kritik von Seiten der Grünen das eben erst geänderte Polizeirecht verschärfen und u. a. die umstrittene Online-Durchsuchung von Computern durchsetzen. Mit den Maßnahmen sollen Terrorpläne vereitelt, politische und organisierte Kriminalität bekämpft sowie häusliche und sexuelle Gewalt verhindert werden. Strobl beteuerte am 22.10.2018, er kenne die Bedenken bezüglich der Online-Durchsuchung: „Trotzdem müssen wir darüber sprechen. Ich bitte um Verständnis, dass ich angesichts der Terrorlage, die wir nach wie vor haben, verfassungsrechtliche Spielräume auslote." Die Terrorgefahr sei hoch, daher werde er nicht aufhören, für seine Initiative zu werben. Um Straftaten zu verhindern, soll die Polizei in Zukunft heimlich Computer und Smartphones z. B. auf Fotos, E-Mails, Videos hin durchsuchen können. Hierfür könnte der Bundestrojaner eingesetzt werden, eine Spähsoftware, die immer wieder in der Kritik steht, gegen das Grundgesetz zu verstoßen. Vor dem Bundesverfassungsgericht in Karlsruhe haben mehrere Organisationen deswegen Verfassungsbeschwerde eingereicht. Auf die Urteile will der Innenminister nicht warten.

Vor einem Jahr hatte sich der grüne Koalitionspartner gegen die Online-Durchsuchungen gesperrt. Grünen-Innenexperte Hans-Ulrich Sckerl erklärte: „Die Grünen halten zunächst nichts davon, dass das Polizeigesetz schon wieder verschärft werden soll." Das alte Polizeigesetz sei nicht mal ein Jahr alt. Man wisse noch nicht mal, wie die ergriffenen Maßnahmen gewirkt haben. Bisher ist in Baden-Württemberg die Überwachung von laufender Kommunikation erlaubt. Die Polizei darf E-Mails und Nachrichten bei Messenger-Diensten wie WhatsApp abfangen und mitlesen. Zum Einsatz kam die Methode nach bisherigen Erkenntnissen aber noch nicht.

Der Entwurf für das verschärfte Polizeigesetz sieht weitere Maßnahmen vor. PolizistInnen sollen auch bei Einsätzen im privaten Umfeld sogenannten Bodycams tragen können, also auch in Wohnungen, Arbeits-, Betriebs- und Geschäftsräumen. Die Schulterkameras werden derzeit flächendeckend eingeführt. Damit sollen PolizistInnen filmen können, um Straftaten aufzuklären und sich zu schützen. Bisher gilt das nur für Einsätze in der Öffentlichkeit.

Nicht nur die Grünen, auch der Landesbeauftragte für Datenschutz und Informationsfreiheit, Stefan Brink, hat verfassungsrechtliche Bedenken. Er sieht einen doppelten Tabu-Bruch: „Zum einen würde damit die Unverletzlichkeit der Privatwohnung, wie sie Artikel 13 unseres Grundgesetzes schützt, in Frage gestellt." Zum anderen käme der sogenannte Richtervorbehalt unter Druck. Demnach dürfe grundsätzlich nur ein unabhängiger Richter über einen Eingriff in die Privatsphäre der Wohnung entscheiden, nicht die Polizei. Dass bei unmittelbarem Handlungsbedarf auch die Staatsanwaltschaft diese Entscheidung treffen dürfe, müsse die Ausnahme bleiben.

Laut dem Entwurf soll die Polizei in Zukunft außerdem DNA-Proben nehmen können, um Straftaten zu verhindern. Bei Demos oder strittigen Konzerten sollen umfassende Personenkontrollen möglich sein. Die Polizei soll vereinzelt vorübergehend Menschen festnehmen können, um eine konkrete Gefahr abzuwenden.

Die Landesregierung hatte das Sicherheitsrecht erst ein Jahr zuvor novelliert, um Polizei und Verfassungsschutz neue Befugnisse an die Hand zu geben. Grün-Schwarz steuerte damals vor dem Hintergrund des Terroranschlags auf den Berliner Weihnachtsmarkt von Ende 2016 nach, bei dem zwölf Menschen getötet worden waren. Das Gesetzespaket trat im Dezember 2017 in Kraft (Pläne für ein verschärftes Polizeigesetz in Baden-Württemberg Spähsoftware und Bodycams sollen Polizei stärken, www.swr.de 22.10.2018).

Bayern

Bundestagsopposition klagt in Karlsruhe gegen PAG

Die Bundestagsfraktionen von Linken, Liberalen und Grünen haben das Bundesverfassungsgericht (BVerfG) per abstrakter Normenkontrolle aufgefordert, das neue bayerische Polizeiaufgabengesetz (PAG) zu prüfen. Der „Angriff der CSU" auf das Grundgesetz (GG) müsse verhindert werden, erklärten Vertreter der Fraktionsspitzen am 10.09.2018 bei der Präsentation der Klage in Berlin. Sie rügten, dass Menschen unter Generalverdacht gestellt würden.

Für die Normenkontrolle sind ein Viertel der Mitglieder des Bundestags notwendig, also in diesem Fall ein Antrag von 216 Parlamentariern. Die drei Fraktionen, die von Thorsten Kingreen, Rechtsprofessor aus Regensburg, vertreten werden, mussten sich in das ungewöhnliche Prozessbündnis begeben, weil keine Fraktion allein das für den Antrag nötige Quorum erreicht. Das BVerfG muss nun prüfen, ob das PAG insgesamt mit dem GG vereinbar ist. Einzelne BürgerInnen müssen so nicht wie bei einer traditionellen Verfassungsbeschwerde erst nachweisen, dass sie, etwa durch eine konkrete polizeiliche Maßnahme, von der Novelle individuell betroffen sind.

Inhaltlich beklagen die Abgeordneten vor allem, dass „bei einer drohenden Gefahr" der bayerischen Polizei ein breiter Werkzeugkasten mit schwerwiegenden Eingriffsbefugnissen zur Verfügung steht, von Maßnahmen zur Identitätskontrolle über Platzverweise bis hin zu einer zeitlich unbeschränkten Gefahrenabwehrhaft. Damit dürfe die Polizei auch gegen unbescholtene Bürger schon weit im Vorfeld echter Gefahren und ohne weitere Nachweis vorgehen. Selbst schwerste Grundrechtseingriffe seien dabei nicht mit den notwendigen rechtsstaatlichen Leitplanken versehen, beschweren sich die Volksvertreter. So werde unter niedrigen Voraussetzungen eine Gefahrenabwehrhaft mög-

lich, für die der bayerische Gesetzgeber nicht einmal eine zeitliche Obergrenze gesetzt habe. Ferner würden auch Fahndungsmittel wie „molekulargenetische Untersuchungen“ erlaubt, die die Gefahr begründeten, dass sich das polizeiliche Handeln zunehmend an „ethnischen Kriterien“ orientiere. Es entstehe eine Polizei, in der sich geheimdienstliche mit operativen polizeilichen Befugnisse verbänden. Kingreen erläuterte, dass mit dem wenig konkreten Begriff der „drohenden Gefahr“ anders als bei dem juristischen Begriff der „Gefahr im Verzug“ es keiner Konkretisierung von Personen, Orten und Situationen bedürfe. Es genüge die Annahme, dass eine Person „gefährlich“ sei. Eine solche „sprachliche Ungenauigkeit ist der erste Schritt hin zu unrechtsstaatlichen Zuständen.“

In der Bewertung des Gesetzes sind sich die drei Fraktionen einig. So erklärte Christian Lindner von der FDP, das bayerische Gesetz schaffe keine Balance zwischen Sicherheit und Freiheit, sondern sei „ein Angriff auf die Freiheit“. Die Vorfeldarbeit sei der Polizei ausdrücklich untersagt, es dürfe in Deutschland keine Geheimpolizei geben, so wie diese im PAG möglich gemacht werde. Das BVerfG habe 2016 für den Bereich der Terrorismusbekämpfung Ausnahmen zugelassen, doch habe die CSU die polizeiliche Vorfeldarbeit auf die „Alltagskriminalität“ ausgeweitet. Linken-Chef Dietmar Bartsch betonte, es gehe um die Auseinandersetzung zwischen einem Rechtsstaat und einem Willkürstaat; das PAG fördere eindeutig Letzteren. Das Gesetz senke die Schwelle für Eingriffe in Grundrechte ab; die Polizei erhalte eine „Kontrollkompetenz“, wie es das seit 1945 nicht gegeben habe. Grünen-Fraktionschefin Katrin Göring-Eckardt erklärte: „Das Gesetz stellt Bürgerrechte infrage.“ Mit einem kleinen Seitenhieb auf ihren Vorredner meinte sie, das PAG erinnere sie an die DDR. Dort hätte die Polizei einen auch immer und überall kontrollieren dürfen, ob mit oder ohne Anlass“. Die Antragstellenden hätten eine „Allianz für den Rechtsstaat“ gebildet; der Rechtsstaat sei bei der CSU „nicht mehr in guten Händen“. Mit deren Plänen gerate jeder unter Generalverdacht; das mache aus „einer Polizei der Bürger eine Polizei des Staates“.

Das neue PAG steht auch in der Kritik wegen der damit ermöglichten weiten Eingriffe in den Telekommunikationsbereich und den verdeckten Zugriff auf IT-Systeme. So wird den Ermittlern auch präventiv der Einsatz von Staatstrojanern für die Quellen-Telekommunikationsüberwachung sowie für heimliche Online-Durchsuchungen gestattet. Diese Aspekte werden in der Klage ebenfalls angeführt. Gegen die Kategorie der „drohenden Gefahr“ als Kriterium polizeilichen Handelns, die in Bayern schon seit einer früheren PAG-Reform 2017 herangezogen werden kann, wurde von den Grünen bereits beim Bayerischen Verfassungsgerichtshof eine Beschwerde eingereicht (vgl. DANA 1/2018. 11-25; DANA 3/2018, 149 f.; Krempl, Bayerisches Polizeigesetz: Opposition legt Verfassungsbeschwerde ein, www.heise.de 10.09.2018; Braun, Ein ungewöhnliches Trio, SZ 11.09.2018, 6).

Berlin

Senat: Videovolksbegehren ist unzulässig

Der rot-rot-grüne Berliner Senat hält das von einer Initiative angestrengte Volksbegehren für mehr Videoüberwachung für unzulässig und hat dieses zur endgültigen Entscheidung dem Berliner Verfassungsgerichtshof vorgelegt (vgl. DANA 2017, 159 f.). Innensenator Andreas Geisel (SPD) erklärte am 16.10.2018, das Vorhaben sei „rechtlich unzulässig und politisch verfehlt“. Der Plan der Initiatoren, Kameras an bis zu 50 Stellen in Berlin aufzuhängen, hätte einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht zur Folge. Der Senat wirft dem Volksbegehren unklare Begriffe vor. So sollen unter anderem große Fahrrad-Abstellplätze und belebte Orte mit Kameras überwacht werden. Man könne den Gesetzentwurf so lesen, dass auch Eingangsbereiche von Krankenhäusern, Schulen und Kirchen überwacht werden sollten. Die Regelung sei unverhältnismäßig, unkonkret und irreführend.

Die Initiatoren des Begehrens wollten mit der Ausdehnung der Videoüberwachung nach eigenen Angaben die Kriminalität eindämmen und das Sicherheitsgefühl der BürgerInnen verbessern. Zu den Initiatoren gehören der frühere Berliner Justizsenator und jetzige CDU-Bundestagsabgeordnete Thomas Heilmann und der ehemalige Neuköllner Bezirksbürgermeister Heinz Buschkowsky (SPD). Im Februar hatte das Bündnis mehr als 25.000 Unterschriften von UnterstützerInnen an die Innenverwaltung übergeben.

CDU-Fraktionschef Burkard Dregger kritisierte den Vorlagebeschluss: „Der Senat hat Angst vor dem Volk.“ Der Beschluss sei ein juristischer Trick, um eine Abstimmung gleichzeitig mit der Europawahl zu verhindern. Er warf dem Senat vor, auf Zeit zu spielen. Er verwies darauf, dass die Berliner Verkehrsbetriebe (BVG) mit ihrer Videoüberwachung in U-Bahnhöfen, Waggons und Bussen erfolgreich seien: „Es ist völlig absurd zu behaupten, dass die bewährte Praxis im Bereich der BVG nicht auch am Kottbusser Tor, am Alex und anderen Kriminalitätsschwerpunkten erlaubt sein soll.“ FDP-Innenexperte Marcel Luthe forderte, die Zahl der PolizistInnen und Feuerwehrleute an die wachsende Stadt anzupassen und um 15% zu erhöhen: „Eine Kamera schützt niemanden“ (Berliner Senat will Video-Volksbegehren stoppen, www. rbb24.de 16.10.2018; Gegen Video-Volksbegehren, SZ 17.10.2018, 5).

Hamburg

Datenschutzbeauftragter beanstandet polizeiliche Gesichtserkennung

Der Hamburgische Datenschutzbeauftragte Johannes Caspar hat den Einsatz biometrischer Gesichtserkennung durch die Polizei bei der Fahndung nach Randalierern zum G20-Gipfel im Juli 2017als rechtswidrig beanstandet. In einem am Freitag 31.08.2018 veröffentlichten Prüfbericht stellt er fest, dass die Ermittlungsbehörden „mathematische Gesichtsmodelle einer unbegrenzten Anzahl von in der Masse verdachtslos erfassten“ BürgerInnen im Stadtgebiet erzeugt, diese für einen unbestimmten Zeitraum gespeichert und damit tief in das informationelle Selbstbestimmungsrecht der Betroffenen eingegriffen haben. Hierfür wäre

eine besondere gesetzliche Befugnis nötig gewesen.

Mit der von der Sonderkommission Schwarzer Block verwendeten Software Videmo 360 seien im Echtzeitbetrieb „ausnahmslos alle Gesichter von Menschen, die sich auf dem umfangreichen Video- und Bildmaterial befanden, biometrisch verarbeitet" worden. Die Technik eröffne Wege zur Fahndung und Überwachung von Personen, „die das menschliche Auge bei Weitem nicht leisten kann". Kriminaltechnisch erschließe sich Strafverfolgern so „eine neue Dimension staatlicher Ermittlungs- und Kontrolloptionen". Überall dort, wo Bildmaterial des öffentlichen Raumes zur Verfügung stehe, könne es künftig zu einer „umfassenden Profilbildung von Menschen" kommen. Darüber sei es möglich, Standorte von einzelnen Personen zu rekonstruieren oder Beziehungen zu anderen Menschen zu dokumentieren: „Mit der automatisierten Gesichtserkennung wird in Hamburg … eine neue Technologie im Echtzeitbetrieb eingeführt, deren Einsatz die gesetzlich austarierte Balance zwischen informationeller Selbstbestimmung und staatlichen Eingriffsbefugnissen zur Strafverfolgung massiv zu Lasten der Privatsphäre von Bürgerinnen und Bürgern verschiebt."

Diese Informationen ermöglichten Schlüsse auf Verhaltensmuster und Präferenzen des Einzelnen. Die mit der Herrschaft über die Bilder erreichte neue Intensität staatlicher Überwachungseingriffe sei „hoch missbrauchsgefährdet". Der Datenschützer geht davon aus, dass die Polizei den Einsatz der Erkennungssoftware nun stoppt. Sonst folge eine formelle Anordnung. Dagegen könne die Innenbehörde dann gerichtlich vorgehen. Ein Polizeisprecher erklärte dagegen, die Anwendung sei unter Beachtung aller rechtlicher Vorgaben erfolgt. Die Strafverfolgungsbehörde hatte jüngst noch angekündigt, das eigens angeschaffte Programm dauerhaft nutzen zu wollen, um Personen zu identifizieren. Caspar hat die Polizei zudem aufgefordert, die „ohne Rechtsgrundlage erhobenen biometrischen Daten" zu löschen. Der Soko liegen über 100 Terabyte Bild- und Videomaterial rund um die Gipfel-Krawalle vor. Die Resultate der biometrischen Fahndung waren bisher eher dürftig (Krempl, G20-Krawalle: Datenschützer rügt Fahndung per automatisierter Gesichtserkennung, www.heise.de 31.08.2018; Caspar kritisiert Software zur Gesichtserkennung, Kieler Nachrichten 01.09.2018, 14).

Hessen

Datenschutzgrundrechte in der Landesverfassung

Bei einer parallel zur hessischen Landtagswahl am 28.10.2018 erfolgten Volksabstimmung haben die WählerInnen nicht nur die Todesstrafe im Lande formell abgeschafft, sondern mit 90,9% auch ein Grundrecht auf Datenschutz in der Verfassung des Landes verankert. In Artikel 12a heißt es nun: „Jeder Mensch ist berechtigt, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen." Damit wird das 1983 vom Bundesverfassungsgericht (BVerfG) mit dem Volkszählungsurteil abgeleitete Recht auf informationelle Selbstbestimmung, ausdrücklich normiert. Weiter heißt es: „Die Vertraulichkeit und Integrität informationstechnischer Systeme werden gewährleistet." Damit wird in Hessen auch das noch vergleichbar junge, 2008 vom BVerfG in Karlsruhe abgeleitete IT bzw. Computer-Grundrecht kodifiziert. Einschränkungen der neuen Rechte bedürfen eines Gesetzes, heißt es in dem Artikel. Der hessische Landtag hatte die Initiative unter anderem damit begründet, dass die Privatsphäre von Einzelnen beim Nutzen von IT-Systemen vor allem durch heimliche Zugriffe etwa über Spähprogramme gefährdet sei. Es bestehe damit „ein Bedürfnis für besonderen Schutz".

Auf Bundesebene drängten die Grünen im Bundestag 2008 darauf, ein Datenschutzgrundrecht festzuschreiben. Das Recht auf Privatheit müsse zunehmend gegen den Staat und gegen die Wirtschaft verteidigt werden. Es sei wünschenswert, dass die Bürger ihre grundlegenden Rechte aus dem Grundgesetz selbst auch im Bereich der neuen Technologien in hinreichender Klarheit entnehmen könnten. Die damalige Justizministerin Brigitte Zypries (SPD) tat die Initiative als Symbolpolitik ab. Ob die Kodifizierung tatsächlich etwas bringt, ist umstritten. Zudem gilt seit 2009 auf europäischer Ebene ein präziser formuliertes Grundrecht auf Datenschutz in Art. 8 der Grundrechte-Charta. Was die Festschreibung des Computergrundrechts über die auch heute noch wirksame Symbolik hinausgehend bringen wird, bleibt abzuwarten (Krempl, Hessen: Grundrecht auf Datenschutz und digitale Infrastruktur, www.heise.de 02.11.2018).

Niedersachsen

Grünen-Beschwerde wegen Landesdatenschutzgesetz

Die Grünen im niedersächsischen Landtag haben sich an die Kommission der Europäischen Union (EU) gewandt mit dem Hinweis darauf, dass das neue niedersächsische Datenschutzgesetz in einzelnen Punkten mit der europäischen Datenschutz-Grundverordnung (DSGVO) nicht in Einklang steht. Der innenpolitische Sprecher der Grünen-Fraktion Belit Onay erklärte: „Die Große Koalition hat ohne Not in unfassbarer Eile ein Gesetz in Rekordtempo durch das Parlament gepeitscht und dabei sehenden Auges europa- und verfassungsrechtliche Verstöße in Kauf genommen. Das war angesichts der massiven Kritik der Rechtsexperten schon fast ein böswilliger Vorgang." Die Erlaubnis von Überwachungskameras im öffentlichen Raum habe eine „ausufernde Ausweitung" erfahren. Der Landesdatenschutzbeauftragten würden nur mangelnde Kontrollrechte zugestanden. So sei bei Strafverfahren eine Datenschutzkontrolle erst nach deren Abschluss zulässig. Die Staatsanwaltschaften seien vom Anwendungsbereich des Gesetzes ganz ausgeschlossen. Überdies habe die Datenschutzbeauftragte auch keine Befugnis, Bußgelder gegen öffentliche Stellen zu verhängen, die gegen die DSGVO verstoßen. Dazu kämen handwerkliche Mängel des vom Innenministerium erarbeiteten Gesetzes: „Die Umsetzung der europarechtlichen Vorgaben ist vielfach bestenfalls Stückwerk." Die Landesdatenschutzbeauftragte Barbara Thiel hatte zuvor den dann beschlossenen Gesetzentwurf mehrfach kritisiert. Während des Parlamentsverfahrens hatten neben FDP und Grünen auch mehrere Verbände Mängel beklagt. Da die landespolitischen Möglichkeiten ausgeschöpft

seien, müssten die Grünen, so Onay, nun die EU einschalten: „So einfach werden wir die GroKo mit dieser Nummer nicht durchkommen lassen." Niedersachsen dürfe „nicht zur Datenschutzwüste Europas" verkommen (Datenschutz: Grüne reichen Beschwerde gegen Niedersachsens Datenschutzgesetz ein, wallstreet-online.de 28.08.2018; siehe dazu auch die ausführliche Kritik an dem Gesetz durch das Netzwerk Datenschutzexpertise, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/br_2018_ndsdsg02.pdf).

Niedersachsen

Deutscher spioniert für jordanischen Geheimdienst

Die Bundesanwaltschaft hat einen 33 Jahre alten Deutschen festnehmen lassen, der für den jordanischen Geheimdienst spioniert haben soll. Alexander B. habe, so die Karlsruher Behörde, den Auftrag gehabt, Informationen über eine als Radikalen-Treff bekannte Moschee in Hildesheim zu sammeln. Das niedersächsische Innenministerium hatte den Verein „Deutschsprachiger Islamkreis Hildesheim" (DIK) im März 2017 verbieten und dessen Moschee versiegeln lassen. Die Sicherheitsbehörden hatten Erkenntnisse, dass dort Kämpfer für die Terrororganisation „Islamischer Staat" (IS) im Irak und in Syrien rekrutiert wurden. Auch Anschlagspläne in Deutschland seien ins Auge gefasst worden. Der Festgenommene soll seinen Auftraggebern Informationen über mehrere Personen geliefert haben, die in den Dschihad ziehen und nach Syrien ausreisen wollten oder sich schon dort aufhielten. Der Mann wurde dem Haftrichter vorgeführt und sitzt in Untersuchungshaft (Deutscher soll für jordanischen Geheimdienst spioniert haben, www.spiegel.de 08.08.2018).

Nordrhein-Westfalen

Wegen „Datenschutz" kein Bastelsieger

In Solingen ist ein Mal- und Bastelwettbewerb schiefgegangen, weil die Organisatoren vom Naturschutzbund (Nabu) aus Gründen des Datenschutzes zu datensparsam vorgegangen sind: Weil nur die Vornamen der kleinen KünstlerInnen notiert wurden, konnten die SiegerInnen nicht benachrichtigt werden: In den Sommerferien hatte der Nabu Kinder zur Teilnahme an dem Wettbewerb aufgerufen. Die Vorsitzende des Solinger Vereins notierte aber lediglich die Vornamen, auch um den Regeln der neuen EU-Datenschutz-Grundverordnung gerecht zu werden. Sie gab den Kindern stattdessen Visitenkarten mit der Bitte an die Eltern mit, sich zu melden, doch kaum jemand antwortete (DSGVO: Keine Bastelsieger, SZ 28.09.2018, 8).

Rheinland-Pfalz

Video zur Baustellenüberwachung geht viel zu weit

Bei einer Kontrolle einer Baustellenüberwachung war der rheinland-pfälzische Landesdatenschutzbeauftragte Dieter Kugelmann wenig begeistert. Um Diebstähle zu verhindern und den Baufortschritt zu dokumentieren, ließ ein Bauunternehmen Videokameras auf mehreren Baustellen installieren. Die Bilder wurden unter anderem in HD-Qualität live ins Netz übertragen und waren dort auch dauerhaft abrufbar.

In einer ersten Stellungnahme wies Kugelmann darauf hin, dass in den Videoaufnahmen unter anderem auf den Baustellen im Einsatz befindliche Handwerker, Bauleiter und Architekten zu sehen waren. Es wurden also personenbezogene Daten verarbeitet, was einer Rechtsgrundlage bedarf: „Diese erfordert seitens des Bauunternehmers ein berechtigtes Interesse an der Videoüberwachung, das die Interessen der betroffenen Personen, nicht überwacht zu werden, überwiegt." Dabei müssten insbesondere die Belange des Beschäftigtendatenschutzes berücksichtigt werden. Sämtliche Arbeitsabläufe der Beschäftigten ließen sich so überwachen. Mittlerweile sind die Bilder nicht mehr im Internet abrufbar. Abgehakt ist der Fall damit nicht. Das Verfahren ist, so die Landesdatenschutzbehörde, noch nicht abgeschlossen.

Baustellenüberwachung kann zulässig sein, wenn die Persönlichkeitsrechte der Betroffenen gewahrt bleiben. Dem rheinland-pfälzischen Landesdatenschutzbeauftragten zufolge bestehen keine datenschutzrechtlichen Bedenken gegen eine Baustellenüberwachung, wenn 1. lediglich Übersichtsaufnahmen des Baufortschritts angefertigt werden und darauf die Identifizierung der arbeitenden Personen weitgehend ausgeschlossen werden kann, 2. öffentlich-zugänglicher Raum, wie zum Beispiel Nachbargrundstücke und Hausfassaden benachbarter Grundstücke, von der Erfassung ausgeschlossen ist, 3. die Kameras erst nach Beendigung der Bautätigkeit in Betrieb gesetzt werden und 4. auf die Videoüberwachung hingewiesen wird, sodass die Transparenzpflichten eingehalten werden, die sich aus der DSGVO ergeben (Leupold, Baustellenüberwachung: Was erlaubt ist und was nicht, www.handwerk.com 24.09.2018).

Sachsen

Haftbefehl von Rechtsradikalen ins Internet gestellt

Am frühen Morgen des 26.08.2018 war der 35-jährige Deutsch-Kubaner Daniel H. auf einem Stadtfest in der Chemnitzer Innenstadt erstochen worden. Es wurden Haftbefehle gegen zwei Tatverdächtige erlassen, einen 23-jährigen Syrer und einen 22 Jahre alten Iraker. Diese Tat löste gewalttätige Demonstrationen von Rechten und Gegendemonstrationen aus, welche die Stadt über viele Tage erschütterten. Rechtsextreme machten in der Stadt Jagd auf Menschen, von denen sie meinten, dass sie fremder Herkunft sind. Mehrere Rechtsextreme zeigten den Hitlergruß.

Das Dokument im Netz

Angeheizt wurde die Auseinandersetzung dadurch, dass am 28.08.2018 der Haftbefehl gegen einen der Tatverdächtigen unter anderem von Lutz Bachmann, dem Begründer der fremdenfeindlichen Gruppierung Pegida, von der rechten Bürgerbewegung „Pro Chemnitz" und von einem AfD-Kreisverband ins Internet gestellt wurde.

Eine Veröffentlichung erfolgte auch auf der Facebookseite des Bremer Bürgerschaftsabgeordneten Jan Timke. Die Staatsanwaltschaft durchsuchte Timkes Wohnung in Bremerhaven und beschlagnahmte sein Handy, einen Computer und ein Tablet. Timke ist ursprünglich Bundespolizist und Mitglied der rechten Wählervereinigung „Bürger in Wut"; sein Dienstverhältnis ruht, solange er in der Bürgerschaft sitzt.

Die Staatsanwaltschaft Dresden leitete Ermittlungen ein, da, so ein Sprecher, die Weitergabe des geheimen Behördendokuments wie auch die Veröffentlichung strafbar sind. Es sei aber ungewiss, ob sich ermitteln lässt, wer den Haftbefehl weitergegeben hat, da dieser durch die Hände von mehreren Dutzend Behördenmitarbeitenden gegangen ist. Auch Sachsens Justizminister Sebastian Gemkow (CDU) wies darauf hin, dass der Kreis potenziell relativ groß sei. Die Veröffentlichung nannte er „extrem verantwortungslos". In dem Dokument waren Details wie die Namen des Opfers und des Tatverdächtigen und Angaben zum bisher ermittelten Tathergang aufgeführt. Auch Namen von Zeugen wurden veröffentlicht. Es hieß, dass die Staatsanwaltschaft Maßnahmen zu ihrem Schutz ergreifen wolle. Das Dokument trug den Briefkopf des Amtsgerichts Chemnitz, die Unterschrift des Richters, das Aktenzeichen der Staatsanwaltschaft. Der Haftbefehl gegen den 22-jährigen Iraker Yousif A., der zunächst der Tötung des Daniel H. verdächtigt war, wurde am 18.08.2018 vom Amtsgericht Chemnitz aufgehoben; auch die Staatsanwaltschaft sah keinen dringenden Tatverdacht mehr.

Der besondere Schutz von Haftbefehlsangaben

Ein Haftbefehl, der von der Staatsanwaltschaft (StA) bei Gericht beantragt wird, und danach vom Gericht zurück an die StA geht, nimmt einen weiten Weg. Die StA gibt ihn weiter an die zuständige Dienststelle der Polizei; hier war dies die Polizeidirektion Chemnitz. Auch die Justizvollzugsanstalt bekommt eine Ausfertigung, und natürlich auch der betroffene Tatverdächtige über seine anwaltliche Vertretung. Ein Haftbefehl wird traditionell auf Papier verschickt, er wird nicht als Scan in Datenbanken hinterlegt. Doch wandert er durch viele Hände, u. a. von Gerichtsbediensteten und SekretärInnen. Das von Lutz Bachmann geteilte Bild im Netz war kein Scan, sondern ein Foto, das schnell mit einem Smartphone gemacht worden war.

Bundesinnenminister Horst Seehofer (CSU) nannte den Vorgang „vollkommen inakzeptabel". Es könne nicht sein, dass „hochpersönliche Dinge, aber auch interne Abläufe der Justiz" öffentlich würden. „Da muss man alle Möglichkeiten prüfen, die dem Rechtsstaat zur Verfügung stehen". Sachsens stellvertretender Ministerpräsident Martin Dulig (SPD) sprach von einem Skandal: „Da haben wir ein dickeres Problem aufzuarbeiten." Es müsse klar werden, dass bestimmte Sachen in der Polizei nicht mehr geduldet werden. Es könne nicht sein, „dass Polizeibeamte denken, sie könnten so etwas durchstechen, obwohl sie genau wissen, dass sie damit eine Straftat begehen".

Die Auflösung

Die Aufklärung des konkreten Vorgangs ging schneller als vermutet: Am 30.08.2018 wurde bekannt, dass der Haftbefehl von einem Dresdner Justizvollzugsbeamten fotografiert und verbreitet wurde. Dieser bekannte sich dazu in einer von seinem Anwalt verbreiteten Erklärung. Der Beamte hatte das Schriftstück mit seinem Handy fotografiert, als das Dokument nach der Einlieferung des Irakers in die Justizvollzugsanstalt noch im Zugangsbereich lag. Er gab gegenüber der Boulevardpresse an, dass er das Foto später an Kollegen, Freunde des Opfers und an die rechtspopulistische Bürgerbewegung „Pro Chemnitz" verschickt habe. Am 29.08.2018 hätten Polizeibeamte seine Wohnung und die von Kollegen durchsucht und Handys beschlagnahmt. Da sei ihm klargeworden, dass er sich offenbaren müsse. Er wurde umgehend vom Dienst suspendiert.

Wegen der Veröffentlichung des Haftbefehls erfolgten wenig später Durchsuchungen der Fraktionsräume von Pro Chemnitz im Rathaus, von drei Wohnungen und in einer Anwaltskanzlei. Drei Beschuldigten wird demnach vorgeworfen, eine Kopie des Haftbefehls auf einer Facebookseite veröffentlicht zu haben.

Mit der Veröffentlichung des Haftbefehls setzte sich Lutz Bachmann nicht zum ersten Mal mit angeblich besonders guten Kontakten in Sicherheitskreise in Szene. Am 19.12.2016, kurz nach dem tödlichen Anschlag des Tunesiers Anis Amri auf den Berliner Weihnachtsmarkt, twitterte Bachmann: „Interne Infos aus Berliner Polizeiführung: Täter tunesischer Moslem." Erst einen Tag später sprach die Polizei offiziell von Amri als Verdächtigem.

Bachmann und weitere Veröffentlichende im Internet dürften wegen der Verletzung eines Dienstgeheimnisses nach § 353b Strafgesetzbuch (StGB) strafrechtlich zu belangen sein. Solange ein Verdächtiger wie der 22-jährige Iraker sich noch nicht vor Gericht verteidigen konnte, soll er in der Öffentlichkeit nicht vorverurteilt werden, deshalb ist das Veröffentlichen eines Haftbefehls strafbar nach § 353d Nr. 3 StGB. Nach dem Amri-Attentat im Jahr 2016 war Bachmann zurückgerudert: „Liebe Presse, ich gebe es zu, ich hatte natürlich nur meine Glaskugel und keinen Informanten!". Diese Ausflucht ist diesmal nicht möglich (Schneider, Neue Justizaffäre erschüttert Sachsen, SZ 30.08.2018, 1; Steinen, Das Leck von Chemnitz, SZ 30.08.2018, 6; Billion/Schneider/Rossbach, Kretschmer verspricht mehr Härte gegen Rechte, SZ 31.08.2018, 1; Durchsuchung im Rathaus SZ 11.09.2018, 6; Grill/Wiegand, Ein Verdächtiger von Chemnitz ist wieder frei, SZ 19.09.2018, 5).

Sachsen u. a.

Rechtsextreme mit „Datenschutz" gegen die Presse

Die Mitglieder von Pegida betrachten sich selbst als „patriotischen Europäer", doch ist für sie zunächst einmal grundsätzlich alles, was aus Brüssel kommt, politisch zu bekämpfende bürokratische Bevormundung. Datenschutz ist für sie ein Fremdwort, etwa wenn es um die Verleumdung der politischen Gegner geht. Doch haben die Rechten bei Bedarf ein sehr instrumentelles Verhältnis zum Datenschutz und zu der im Rahmen der Europäischen Union (EU) erarbeiteten und seit Mai 2018 direkt anwend-

baren Datenschutz-Grundverordnung (DSGVO). So versuchen Pegida-AnhängerInnen und Mitglieder anderer rechter Gruppen mit dem Verweis auf den Datenschutz, die Arbeit von JournalistInnen und BeobachterInnen zu behindern. Sie bedienen sich dabei gerne der Polizei, deren Beamte sich am Ort des Geschehens oft als nicht allzu sattelfest in den sich stellenden juristischen Fragen erweisen.

Demo in Dresden

Ein geradezu klassisches Beispiel hierfür ereignete sich am 16.08.2018, als Bundeskanzlerin Angela Merkel Dresden besuchte. Verglichen mit zurückliegenden Wahlkampfauftritten ging es dabei recht unaufgeregt vonstatten. Etwa 300 Pegida- und AfD-AnhängerInnen hatten sich am sächsischen Landtag verabredet, um gegen die Kanzlerin zu protestieren. Ein Vorfall am Rande der Demonstration führt jedoch zu starken politischen Verwerfungen: Ein Kamerateam des ZDF, das den Besuch Merkels für das Magazin „Frontal 21" begleitete, wurde durch Polizisten an der Arbeit gehindert. Der für Frontal arbeitende freie Journalist Arndt Ginzel wollte gemeinsam mit einem Kameramann die Demonstration dokumentieren. Der Kameramann hatte sich der Versammlung zunächst allein genähert und wurde dann von einem Teilnehmer beschimpft. Ein Mann mit Hut in Deutschlandfarben kam aus dem Hintergrund auf die Kamera zu und rief: „Hören Sie auf, mich zu filmen". Der Kameramann bat ihn, einfach weiterzugehen. Stattdessen kamen weitere Männer hinzu und schlugen nach der Kamera. Wenig entfernt standen Polizisten, die hiergegen nicht eingriffen. Die Polizei hielt vielmehr den Kameramann fest, um dessen Personalien und Presseausweis zu kontrollieren. Ginzel: „Einen Grund für die polizeiliche Maßnahme nannte man uns nicht." Ein Demonstrant, der die Szene aus der Nähe verfolgte, erstattete dann Anzeige gegen Ginzel und gab an, beleidigt worden zu sein, was dieser bestreitet. Er habe der Polizei sogar angeboten, das Filmmaterial vor Ort zu sichten, um den Sachverhalt aufzuklären. Dies sei abgelehnt worden. Auch der Bitte, ihre Namen zu nennen, seien die Beamten während des 45-minütigen Vorfalls nicht nachgekommen. Ginzel veröffentlichte ein den gesamten Vorgang dokumentierendes Video via Facebook und Twitter. Der überwiegend investigativ, auch in der rechten Szene, arbeitende Journalist erklärte: „Die Polizei behindert nicht nur unsere Arbeit, sie bestärkt Pegida-Anhänger in ihrem aggressiven Auftreten gegenüber Journalisten."

Reaktionen

Michael Hiller, Geschäftsführer des Deutschen Journalistenverbands Sachsen, verurteilte das Vorgehen der Beamten, forderte Aufklärung und eine Entschuldigung. Enrico Stange, innenpolitischer Sprecher der Linken im sächsischen Landtag, warf der Polizei vor, als Handlanger von Pegida aufzutreten und verlangte, den Vorfall zum Thema im Innenausschuss zu machen. Valentin Lippmann, innenpolitischer Sprecher der Grünen, erklärte, die Polizei dürfe sich nicht von Gegnern der freien Presse instrumentalisieren lassen. Er sprach sich für mehr Fortbildungsmaßnahmen im Umgang mit Medienvertretern aus. Bundeskanzlerin Angela Merkel (CDU) erklärte während eines Besuchs in Georgien, wer auf eine Demonstration gehe, müsse damit rechnen, dass er „durch Medien dabei aufgenommen und beobachtet wird". Sie bekenne sich „ausdrücklich zur Pressefreiheit", es müsse „eine freie Arbeit der Journalisten geben". Bundesjustizministerin Katarina Barley nannte den „Vorfall in Sachsen so besorgniserregend; die sächsischen Behörden müssen umfassend aufklären."

Dagegen heizte der Chef der CDU-Fraktion im Sächsischen Landtag Frank Kupfer, den Konflikt dadurch an, dass er auf Facebook schrieb: „Öffentlich rechtliche … dafür bezahlen wir Beiträge." Auf heftige Kritik stieß zwei Tage später auch ein Tweet des sächsischen Ministerpräsidenten Michael Kretschmer (CDU), der schrieb: „Die einzigen Personen, die in diesem Video seriös auftreten, sind Polizisten." Hunderte Kommentatoren warfen daraufhin auf sozialen Medien Kretschmer vor, er diskreditiere die betroffenen Journalisten und mache durch seine Äußerung eine unvoreingenommene Untersuchung des Falls unmöglich. Später beteuerte Kretschmer: „Ich bin ein überzeugter Verteidiger der Pressefreiheit." Das sächsische Innenministerium warnte auf Twitter davor, „geschnittene Filme voreilig zu bewerten". Im Falle einer Anzeige müssten Polizisten handeln und Personalien aufnehmen: „Offensichtlich ist genau das geschehen. Nicht mehr und nicht weniger."

Derweil bat die Polizei Sachsen auf ihrem Twitterkanal wegen des Wochenendes um Geduld und teilte mit, dass der Dresdner Polizeipräsident die Journalisten zu einem „klärenden Gespräch" einlade. SPD-Chef und stellvertretender Ministerpräsident Martin Dulig widersprach Kretschmer, der die behinderten ZDF-Journalisten indirekt als unseriös bezeichnet hatte. Am 24.08.2018 räumte Dresdens Polizeipräsident Horst Kretschmar nach einem Treffen mit dem Reporter und Verantwortlichen des ZDF im Gegensatz zu seinem Innenminister Fehler ein, worauf der Sender erklärte: „Das ZDF begrüßt, dass sich der Polizeipräsident in dem offenen Gespräch für die Art und Weise der polizeilichen Maßnahme entschuldigt hat."

Der Mann, der nicht gefilmt werden wollte

Der Mann, in den Medien Maik G. genannt, der so lange gegen Journalisten gepöbelt hatte, bis die Polizei einschritt, entpuppte sich im Nachhinein als im Bereich Wirtschaftskriminalität tätiger Mitarbeiter des sächsischen Landeskriminalamts (LKA). In dieser Funktion hatte er Zugriff auf das polizeiliche Erfassungssystem IVO, in dem alle Straftaten und Ermittlungsvorgänge des Landes registriert werden, sowie auf das nationale Ausländerzentralregister. Gemäß Presseberichten überprüfte das LKA nach der Veröffentlichung des Vorgangs Verbindungen des Manns zur rechten Szene in Freital, insbesondere zu einer dortigen fremdenfeindlichen Bürgerinitiative.

Die Aufzeichnung des Fernsehteams mit ihm, in der er durch eine schwarz-rot-goldene Kappe gut erkennbar ist, wurde zum Kurzfilm-Hit im Fernsehen in Nachrichten- wie in Satiresendungen, im Internet sowie und in der Printpresse. Seinen vehementen Auftritt führten Kollegen u. a. darauf zurück, dass es kurz zuvor im LKA eine Schulung zur DSGVO gegeben habe, die er aber of-

fenkundig falsch verstanden habe. Der Clip zu dem Vorfall wurde im Internet millionenfach geclickt. Am 25.08.2018 erklärte Dulig von der SPD unter Bezugnahme auf öffentlich geäußerte Forderungen, den Mann „aus dem Dienst zu entfernen": „Ich denke, das ist tatsächlich das, was man jetzt überprüfen muss, ob arbeitsrechtliche Konsequenzen zu ziehen sind." Am 30.08.2018 teilte das sächsische LKA mit, dass der Tarifangestellte, der den umstrittenen Polizeieinsatz ausgelöst hatte, nach einem Gespräch mit dem LKA anbot, die Polizei zu verlassen. Er werde „eine andere adäquate Tätigkeit außerhalb der Polizei Sachsen wahrnehmen."

Die Rechtslage

Gemäß der neuen DSGVO sind Fotografen grds. angehalten, Personen vor Ablichtung um Einverständnis zu bitten. JournalistInnen sind aber von der Regelung ausgenommen, für sie gilt das sogenannte Medienprivileg (Art. 85 DSGVO). Nach § 23 des Kunsturhebergesetzes (KUG) dürfen zudem „Bilder von Versammlungen, Aufzügen und ähnlichen Anlässen, an denen die dargestellten Personen teilgenommen haben" auch ohne Einwilligung erstellt und sogar veröffentlicht werden.

Stuttgart

Kurz nach dem Vorfall in Dresden wurde ein Ereignis aus Stuttgart am Rande einer Demonstration bekannt. Dort waren 30 Vertreter der rechtsextremen identitären Bewegung auf 80 Gegendemonstranten gestoßen. Ein Polizeibeamter soll dabei Journalisten den Weg versperrt und geäußert haben: „Die Pressefreiheit ist jetzt ausgesetzt." Baden-Württembergs Innenminister Thomas Strobl (CDU) reagierte darauf prompt: „Wenn diese Worte so gefallen sein sollten, ist das selbstverständlich völlig falsch."

München

In München hatte es kurz zuvor mindestens drei vergleichbare Vorfälle zu dem in Dresden gegeben. Am 06.08.2018 praktizierte die Pegida in München die Taktik. Von der Bühne am Marienplatz kündigte Pegida-Chef Heinz Meyer Anzeigen gegen Fotografen an und verwies auf dabei auf die DSGVO. Der Trick funktionierte: Polizisten nahmen Personalien eines Fotografen auf, eine Speicherkarte wurde sichergestellt, die der Mann nach seinen Angaben zwei Wochen später per Post zurückbekommen hat. Zwei Tage danach gab es einen weiteren ähnlichen Vorfall. Beim Bayerischen Journalisten-Verband (BJV) nahm man die Angelegenheit ernst und intervenierte. Gut eine Woche später veröffentlichte die Münchner Polizei über ihren Sprecher Marcus Da Gloria Martins per Twitter eine Klarstellung. Die DSGVO, der europäische Datenschutz, habe „keine einschränkenden Auswirkungen auf die journalistische Berichterstattung über Versammlungslagen." Das Wort „keine" war unterstrichen. Das Grundrecht auf Pressefreiheit sei ein „elementares Rechtsgut".

Dennoch hatte eine Woche später Pegida mit der Masche erneut Erfolg. Diesmal hatte es die rechte Gruppierung auf die Fachinformationsstelle Rechtsextremismus München (Firm) abgesehen, die Teil des städtischen Netzwerks gegen Rechtsextremismus ist. Firm ließ bei einer Pegida-Versammlung am Stachus Flugblätter in Deutsch und Englisch verteilen, die über die Hintergründe der Gruppierung informieren. Auf dem englischsprachigen Flyer ist am rechten Bildrand ein stämmiger Mann mit Bart und Sonnenbrille zu sehen. Er gehört zum Pegida-Stammpersonal und trat mehrmals als Anmelder der Kundgebungen auf. Nach Medienberichten war der Mann mindestens einmal auch auf einer Patrouille der rechten Bürgerwehr „Soldiers of Odin" (die sich inzwischen in „Wodans Erben Germanien" umbenannt hat) unterwegs.

Der rechte Aktivist stellte nach Firm-Angaben Strafanzeige wegen illegaler Verbreitung personenbezogener Daten. Polizisten nahmen daraufhin die Personalien der Flugblattverteilenden auf. Marcus Buschmüller von Firm: „Durch solche Maßnahmen wird demokratischer zivilgesellschaftlicher Protest behindert und eventuell sogar kriminalisiert." Die Fachinformationsstelle kündigte ihrerseits rechtliche Schritte an.

Dennis Amour, Geschäftsführer des BJVs, erklärte, dass die Vorgehensweise von Rechten Methode habe: Mit „haltlosen Anschuldigungen" würden JournalistInnen an ihrer Arbeit gehindert. Schon Mitte August hatte der Polizeisprecher Da Gloria Martins darauf hingewiesen: „Komplexe und weitreichende Gesetzesänderungen wie die DSGVO erzeugen bei ihrer Einführung in der Praxis immer wieder rechtliche Fragestellungen." Mittlerweile habe es im Präsidium interne Besprechungen zu dem Thema gegeben. Pressesprecher Sven Müller meinte, die Polizei stehe vor einem Dilemma: „Wenn jemand auf eine Anzeige besteht, können wir ihn nicht einfach wegschicken." Es gebe jedoch die Möglichkeit einer bloßen Notiz über den Wunsch, Anzeige zu erstatten, ohne Verfahren und ohne Belehrungen, die dann der Staatsanwaltschaft zugeleitet werde (Nimz, Ministerpräsident im Shitstorm, SZ 20.08.2018, 6; Rietzschel, Mal Freund, am Helfer, Nimz, Debakel mit Hut, SZ 24.08.2018, 2; Rossmann, Merkel verteidigt Pressefreiheit, SZ24.08.2018, 1; SPD-Dulig will LKA-Pegidist entlassen, www.bild.de 25.08.2018; Bernstein, Die Masche mit dem Datenschutz, SZ 25./26.08.2018, 41; Mayr/Nimz, Sachsen-SPD greift CDU an, SZ 25./26.08.2018, 6; Versetzt SZ 31.08.2018, 5).

Thüringen

Schützenbund fordert Infos über Reichsbürger

Bei der seit 2016 Jahren beabsichtigten und bisher wenig erfolgreichen Entwaffnung von Reichsbürgern in Thüringen setzt der dortige Innenminister Georg Maier (SPD) auf verstärkte Unterstützung der Behörden durch Schützenverbände: „Sie sollten beobachten, was Mitglieder von sich geben und schauen, ob vor dem Haus eines Schützenbruders die Reichskriegsflagge weht." Er versicherte zugleich, dass die Schützenvereine des Landes nicht von Reichsbürgern unterwandert seien.

Es gibt jedoch ein Problem mit dem „Datenschutz" beim Entzug der mindestens 115 scharfen Pistolen, Revolver und Gewehre, die in der Thüringer Reichsbürger-Szene kursieren, so Hans Gülland, Vizepräsident des Deutschen Schützenbunds in Thüringen: „Wenn wir von staatlichen Stellen keine konkreten Hinweise auf bestimmte Personen bekommen, haben wir praktisch keine

Möglichkeiten, einzugreifen. Wir wissen nicht, wer Reichsbürger ist. Man sieht es ihnen nicht an. Doch die Informationen, die für uns wichtig wären, dürfen die Behörden uns nicht geben – obwohl das wünschenswert wäre." Zig Mal habe er das Thema mit Spitzenvertretern von Sicherheitsbehörden besprochen: „Aber wir bekommen nicht einmal Informationen, wenn ein Verdacht vorliegt." Der jeweilige Schützenverband, von denen es in Thüringen neun gibt, könnten die jeweiligen „Reichsbürger" ausschließen. Der Verband könnte bei stichhaltigem Verdacht erklären, dem Schützen fehle mit dem Ausscheiden aus dem Verband das Bedürfnis zum Besitz scharfer Waffen: „Das wäre theoretisch eine Möglichkeit", falls die Informationen vorlägen.

Die CDU-Sicherheitspolitiker Raymond Walk und Wolfgang Fiedler gehen sogar von fast 200 legalen scharfen Waffen aus. Walk erklärte: „Es dürfen keine Waffen in der Hand von Extremisten sein. Die Waffenbehörde muss bei der Entwaffnung von Reichsbürgern den rechtlichen Rahmen ausschöpfen." Minister Maier habe das Problem erkannt, allerdings hapere es an der praktischen Umsetzung. „Es darf kein Vertrauen des Staates in Personen geben, die Waffen beantragen. Die Antragsteller müssen nachweisen, dass sie vertrauenswürdig sind."

Der Entzug einer Waffenrechtserlaubnis ist rechtlich kompliziert. Einfacher ist es, die Erlaubnis bei der Antragstellung zu verweigern. Tatsächlich sind Behörden in Thüringen bislang stets vor Gerichten gescheitert, wenn sie Reichsbürgern die waffenrechtliche Erlaubnis wieder entziehen wollten. Aber die Spruchpraxis der Verwaltungsgerichte ist offensichtlich im Wandel. So entschied ein Verwaltungsgericht in Gießen kürzlich, dass Reichsbürger keine Waffen tragen dürften. Dieser Wandel in der Rechtsprechung ist möglicherweise auch darauf zurückzuführen, dass im Oktober 2016 im fränkischen Georgensgmünd ein Reichsbürger einen Polizeibeamten erschoss. Der Schütze, der 2017 wegen Mordes zu lebenslanger Haft verurteilt worden ist, war jahrelang im Schützenverein aktiv und hatte zahlreiche Titel und Spitzenplatzierungen mit großkalibrigen Waffen erzielt. Von den 18.000 Reichsbürgern in Deutschland besitzen nach Erkenntnissen der Ämter für Verfassungsschutz mehr als 1.000 eine waffenrechtliche Erlaubnis. In Thüringen gibt es aktuell etwa 1.100 Reichsbürger, darunter 50 Rechtsextremisten. Mindestens 43 Thüringer Reichsbürger sollen legal im Besitz von Waffen sein (Schauka, Datenschutz erschwert Entwaffnung von Reichsbürgern in Thüringen, www.thueringer-allgemeine.de 22.08.18).

Thüringen

Bußgeldverfahren gegen Regierungschef eingestellt

Ein datenschutzrechtliches Bußgeldverfahren gegen den Regierungschef Thüringens Bodo Ramelow (Linke) wurde eingestellt. Dem Ministerpräsident wurde vorgeworfen, beim Twittern ein Foto seines Justizministers Dieter Lauinger (Grüne) und von Lauingers Frau und Sohn veröffentlicht zu haben. Damit habe Ramelow, so der thüringische Landesbeauftragte für Datenschutz, „vorsätzlich oder fahrlässig" gegen die Datenschutz-Grundverordnung verstoßen. Das veröffentlichte Bild war bei der Abi-Feier von Laubingers Sohn entstanden. Ramelow gratulierte der Familie auf seinem privaten Twitter-Account, was die Opposition in Erfurt erboste. Der Vorgang beschäftigt u. a. einen Untersuchungsausschuss im Landtag. Die Einstellung des Verfahrens erfolgte, nachdem Ramelow eine Einwilligung der Familie vorlegte, in der steht, dass das Foto veröffentlicht werden darf. Dies wollte der Datenschutzbeauftragten aber auf Presseanfrage aus Gründen des Datenschutzes nicht bestätigen (Fahrlässige Tweets, Der Spiegel Nr. 38 15.09.2018, 143).

Datenschutznachrichten aus dem Ausland

Weltweit

Deutsche Regierung: Keine Ahnung über Anti-Doping-Datenverarbeitung

Beim weltweiten Anti-Dopingkampf müssen die AthletInnen etwa drei Monate im Voraus ihre Termine und Aufenthaltsorte angeben, für unangekündigte Probennahmen täglich erreichbar sein und intimste Details wie Krankheitsdaten oder Ergebnisse von Urinproben per Smartphone oder Internetbrowser in eine Datenbank einpflegen. Das biologische Profil von bis zu 2.500 deutschen SpitzensportlerInnen liegt der Nationalen Anti-Doping-Agentur (Nada) und auf internationaler Ebene der Welt-Anti-Doping-Agentur (Wada) vor. Aus einer Antwort der deutschen Bundesregierung auf eine kleine Anfrage der FDP-Bundestagsfraktion ergibt sich, dass sie keine genauere Kenntnis darüber habe, welche Personen auf die Wada-Datenbank „Adams" Zugriff haben. Bezüglich des Datenschutzes zieht sie sich aus der Verantwortung: „Die Einschätzung der Datensicherheit bei Nada und Wada obliegt nicht der Bundesregierung, sondern den zuständigen Aufsichtsbehörden." Man habe „keine Kenntnis" darüber, wie viele Personen auf die Datenbank der Wada Zugriff haben.

Stefan Brink, Datenschutzbeauftragter des Landes Baden-Württemberg, bezeichnet diesen Zustand als unverantwortlich: „Sich auf Unwissenheit zu berufen, ist dem Parlament gegenüber unlauter. Auch gegenüber den betroffenen Sportlern ist die Haltung der Bundesregierung inakzeptabel. Einerseits macht sie die Förderung von Sportlern von einer Unterwerfung unter die Antidoping-Richtlinien der Agenturen abhängig, andererseits beruft sie sich darauf, nicht zu wissen, was dort mit den Daten der Sportler passiert."

Die Anfrage bezieht sich nicht nur auf die Datenschutzrichtlinien der Nada, die in Bonn sitzt, sondern auch auf die der Wada, für die das kanadische Datenschutzrecht gilt. Die Bundesregierung erklärte, „keine Kenntnis" über die Details des Wada-Berechtigungskonzeptes zu haben. Mehrfach zieht sie sich darauf zurück, für die Tätigkeit der internationalen Verbände nicht verantwortlich zu sein. Dazu Brink: „Formal mag dies zutreffen, in der Sache steuert die Bundesregierung alleine durch die Mittelvergabe im Sport- und Anti-Doping-Bereich aber wesentlich mit." Das Inkrafttreten der neuen Datenschutzgrundverordnung (DSGVO) im Mai 2018 hat nach Ansicht der Bundesregierung keine direkten Auswirkungen. Brink sieht dies anders: „Ich halte es nicht für zutreffend, dass die Verarbeitung von Sportlerdaten durch die Wada nicht unter die DSGVO fällt." Es handele sich um Daten von betroffenen Personen, die sich in der Europäischen Union befinden. Formal rechtlich handelt die Nada korrekt: Sie verarbeitet Sportlerdaten auf Grundlage der Paragraphen 9 und 10 des Anti-Doping-Gesetzes. Bezüglich der Speicherfrist der Athleten-Daten teilt die Bundesregierung mit, dass diese „zwischen 18 Monaten und zehn Jahren" liege. Ob und wann Daten gelöscht werden, ob AthletInnen gar ein Löschrecht besitzen, darüber habe sie keine Kenntnis.

Die russische Hackergruppe „Fancy Bear/APT28" hatte sich 2016 Zugang zur Datenbank „Adams" verschaffen können. Obwohl auch Daten von deutschen AthletInnen veröffentlicht wurden, sieht die Bundesregierung die Mitwirkung der AthletInnen am „Adams"-System uneingeschränkt und nach wie vor als verpflichtend an (Balleer, Anti-Dopingkampf: Bundesregierung gibt Wissenslücken beim Datenschutz zu, rp-online.de 04.07.2018).

Europa

Once-Only kommt

Der Ministerrat der Europäischen Union (EU) hat am 27.09.2018 ohne weitere Aussprache dem Verordnungsentwurf für ein zentrales europäisches Online-Verwaltungsportal, das nach dem „Once-only"-Prinzip arbeiten soll, zugestimmt und damit den Weg hierfür freigemacht. Die Verhandlungsführer der Mitgliedsstaaten hatten sich zuvor im Juni mit Vertretern des EU-Parlaments auf eine gemeinsame Linie geeinigt. Die Verordnung muss damit nur noch unterzeichnet werden und tritt zwanzig Tage nach der Veröffentlichung im EU-Amtsblatt in Kraft.

Über das seit Mitte 2017 geplante digitale Zugangstor sollen BürgerInnen und Unternehmen einfacher grenzüberschreitend auf E-Government-Dienste der Ämter in der gesamten EU zugreifen können. Einige „grundlegende Verwaltungsangebote", die in einem Mitgliedsland verfügbar sind, werden dabei künftig auch von Personen und Firmen anderer EU-Länder direkt nutzbar sein. BürgerInnen sollen EU-weit per Mausklick etwa einen Wohnsitznachweises, Studienbeihilfen oder eine Krankenversicherungskarte beantragen, ein Kraftfahrzeug zulassen, Rentenleistungen in Anspruch nehmen oder sich in Renten- und Krankenversicherungssysteme registrieren sowie akademische Titel anerkennen lassen.

Um die Bürokratie zu verringern, gilt für das Portal der „Grundsatz der einmaligen Erfassung" (once only). BürgerInnen und Unternehmen sollen die gleichen Auskünfte gegenüber den öffentlichen Verwaltungen also nur einmal abgeben müssen. Der EU-Datenschutzbeauftragte Giovanni Buttarelli hatte anfangs bei diesem vorgesehenen Once-only-Prinzip Datenschutzbedenken vorgetragen. Er zweifelte etwa die Vereinbarkeit mit den Prinzipien der Zweckbestimmung und der Datensparsamkeit an.

Das übergreifende Portal soll in das bereits bestehende Angebot „Ihr Europa" integriert werden mit einer speziellen neuen Nutzerschnittstelle, die in allen EU-Amtssprachen verfügbar ist. Das Interface werde „den uneingeschränkten Zugang zu Online-Verfahren in diskriminierungsfreier Weise gewährleisten". Ein Grundprinzip sei es, dass ein Verfahren, das BürgerInnen eines Mitgliedslands zur Verfügung steht, auch von anderen EU-Staaten aus zugänglich sein soll. Der Betrieb werde durch technische Instrumente unterstützt, die von der EU-Kommission „in enger Zusammenarbeit mit den nationalen Verwaltungen entwickelt werden".

Damit die betroffenen Behörden ausreichend Zeit zur Anpassung ihrer Systeme haben, gelten verschiedene Übergangsfristen. Je nach Sachverhalt müssen die Verfahren und Informationen binnen zwei bis fünf Jahren online verfügbar sein, nachdem die Verordnung in Kraft getreten ist. Hierzulande haben Bund und Länder eine Beta-Version eines E-Government-Portalverbunds gestartet. Das Projekt dürfte auf Basis der neuen EU-Vorgaben deutlich erweitert werden müssen (Krempl, EU-Verwaltungsportal: Bürger müssen Behörden Auskünfte nur noch einmal geben, www.heise.de 28.09.2018).

Österreich

Wien anonymisiert Klingelschilder

In Wien verlieren 220.000 MieterInnen die Namensschilder an ihren Türklingeln. Ein Mieter einer Gemeindewohnung hatte sich über mangelnden Datenschutz beschwert und habe, so ein Sprecher der kommunalen Hausverwaltung „Wiener Wohnen", auf die Datenschutz-Grundverordnung (DSGVO) verwiesen, die im Mai 2018 wirksam wurde. Der Mieter behauptete, nach der EU-Verordnung sei seine Privatsphäre nicht genügend geschützt, wenn sein Name auf dem Klingelschild stehe. Auf die Erkundigung von „Wiener Wohnen" hin erhielt die Hausverwaltung von der für Datenschutzangelegenheiten der Stadt zuständigen Magistratsabteilung die Einschätzung, dass die Verbindung von Nachname und Wohnungsnummer gegen die DSGVO verstoße. Der Sprecher erklärte: „Wir müssen die standardgemäße Beschilderung also austauschen." In 220.000 Wohnungen in rund 2.000 Wohnanlagen sollen bis Ende des Jahres 2018 alle Namen an den Klingelschildern entfernt werden. Stattdessen will die Hausverwaltung Nummern an den Klingelschildern anbringen, damit BesucherInnen immer noch bei der richtigen Wohnung klingeln können. Wer dennoch seinen Namen auf dem Klingelschild haben will, muss dann selbst tätig werden und einen eigenen Aufkleber anbringen. Die Hausverwal-

tung aber dürfe das offiziell nicht mehr erledigen. Medien verbreiteten daraufhin die Ansicht, eine Verpflichtung zur Anonymität bestehe in Österreich eigentlich nicht erst, seitdem die DS-GVO innerhalb der EU gilt. Auch vorher schon habe es ein Recht der Mieter auf Anonymität gegeben, die aber offenbar nicht so streng gesehen und von niemandem bisher eingefordert wurde. Tatsächlich wird in Wien weniger Wert auf einen Namen am Türschild gelegt; es reichen Adresse, Stiege und Wohnungsnummer, damit sich Briefträger zurechtfinden. In Österreich reicht die Tradition der Türnummern bis ins Jahr 1777 zurück. „Top" (vom griechischen Topos – Ort) ist seit den Neunzigern das übliche Wort dafür. Auch in Frankreich, Spanien und den USA ist es seit Jahren üblich, die Klingelschilder von Mehrfamilienhäusern mit Nummern statt mit Namen zu versehen. In Polen gilt mittlerweile die Wohnungsnummer als das einzig verlässliche Identifikationsmerkmal; der Name an der Tür fehlt oft.

Der Datenschutzbeauftragte von Thüringen befeuerte die Diskussion, indem er vor einer Anbringung des Namens durch den Vermieter warnte. Der deutsche Immobilien-Eigentümerverband Haus und Grund empfahl nun seinen 900.000 Mitgliedern, die Namensschilder an vermieteten Wohnungen abzunehmen, was die Bild-Zeitung zu der Überschrift brachte: „Datenschutz-Irrsinn. Unsere Klingelschilder sollen weg!" Die bayerische Datenschutzaufsicht sah dagegen keinen Handlungsbedarf. Gerold Happ, Hausjurist und Mitglied der Bundesgeschäftsführung von Haus und Grund klagte daher: „Das gibt doch keine Rechtssicherheit!" Juristisch wasserdichte Regeln müssten her. Tatsächlich besteht in Deutschland oder in Europa keine Pflicht, die eigenen Wohnung mit dem Namen zu kennzeichnen. Und die Nachfrage im Büro des EU-Kommissionspräsidenten in Brüssel ergab: „Die Datenschutz-Grundverordnung regelt gar nichts zum Thema Namen auf Türklingeln oder Briefkästen. Jeder der was anderes behauptet, liegt falsch." Neben dem Schutz von Daten gebe es auch ein legitimes Interesse zu wissen, wer in einer Wohnung wohnt. Bußgelder würden deshalb nicht verhängt. Dem schloss sich die deutsche Bundesbeauftragte für den Datenschutz an: „Die Aufforderung zur Entfernung sämtlicher Klingelschilder ist unnötig".

Die Leiterinnen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) Marit Hansen und Barbara Körffer präzisierten: „Eine Einwilligung der Mieter ist nicht erforderlich. Vermieter, die eine Beschilderung an der Wohnungsanlage gestalten und für ihre Mieter Klingelschilder anfertigen wollen, können sich auf ein berechtigtes Interesse berufen: Dass die Namen der Mieter dort genannt werden, liegt nicht nur im Interesse der Mieter, die besucht werden oder Postzustellungen oder Lieferungen erhalten wollen, sondern dient auch dem Einsatz von Rettungskräften oder der Polizei. Es entspricht auch den vernünftigen Erwartungen der Mieter. Wichtig ist aber, dass die Vermieter schutzwürdige Interessen der Mieter berücksichtigen müssen, die im Einzelfall bestehen. Das ist ganz deutlich im Fall eines Stalking-Opfers: Wer gerade seine Wohnung wechseln musste, weil er oder sie vorher einem Stalking ausgesetzt war, muss vielleicht um Leib und Leben fürchten – hier sollte man nicht den vollständigen Namen angeben. Natürlich gilt dies auch für Zeugenschutzprogramme.

Wenn nicht ohnehin die Mieter für ihr eigenes Klingelschild zuständig sind, ist es auf jeden Fall sinnvoll, dass der Vermieter vorab die Mieter über die Planungen für ein bereit gestelltes Klingelschild informiert, damit die korrekte Schreibweise des Namens kontrolliert wird oder bevorstehende Namensänderungen, z. B. nach einer Heirat oder Scheidung, sofort umgesetzt werden, damit bei mehreren Mitbewohnern entschieden werden kann, welche Namen aufgeführt werden, damit bei Namensdopplungen abgekürzte oder vollständige Vornamen ergänzt werden können" (220.000 Mieter bekommen Klingelschilder ohne Namen, www.spiegel.de 12.10.2018; Zips, Wie mein Name an der Tür, SZ 19.10.2018, 12; PE BayLDA 18.10.2018, Klingelschild und Datenschutz; PE ULD 19.10.2018, Klingelschild kein Datenschutzverstoß – von der Mücke zum Elefanten).

Österreich

Score berechnet Förderchancen am Arbeitsmarkt

In Österreich werden die Arbeitsmarktchancen von Arbeitssuchenden ab 2020 als verbindlicher Teil der Beratung von einem Computerprogramm des Arbeitsmarktservices (AMS) ausgerechnet: Wer danach mit 66% Wahrscheinlichkeit innerhalb von sieben Monaten wieder einen Job haben wird, soll als Person mit hoher Arbeitsmarktchance gelten. Wem weniger als 25% Chance errechnet werden, innerhalb von zwei Jahren einen Job zu bekommen, gilt dann als Kunde mit niedrigen Chancen. In beiden Kategorien soll es weniger Förderungen als in der mittleren Kategorie geben. In das System werden verschiedene persönliche Kenndaten eingegeben, u. a. die erlangte Ausbildung sowie das bisherige Arbeitsleben. Alter, Geschlecht und Staatsangehörigkeit spielen eine Rolle. Damit sollen Kosten eingespart werden, da „arbeitsmarktpolitische Interventionen vergleichsweise teuer" seien. Die AMS-Beschäftigten setzen das System vom 15.11.2018 an ein. Der vormalige Sozialminister Alois Stöger (SPÖ) verhinderte im Herbst 2016 wegen Bedenken den Einsatz eines derartigen Computerprogramms. Seine Begründung damals: Mit dem System würden perspektivlose Arbeitssuchende künftig weniger gefördert.

In einem Dokument, das der AMS zu dem Programm veröffentlichte, ist nachzulesen, welche Eigenschaften der Algorithmus als negativ oder positiv bewertet. Der Einsatz des Systems dürfte zur Folge haben, dass Frauen, Ältere, gesundheitlich Beeinträchtigte und Frauen mit Kindern vom Computerprogramm automatisch schlechter eingestuft werden. Hat eine Frau ein Kind und dadurch entsprechende Betreuungspflichten, kriegt sie vom AMS-Algorithmus Extra-Punkteabzüge, Männer mit Betreuungspflichten jedoch nicht. Michael Wagner-Pinter von der Firma Synthesis Forschung GmbH, die hinter dem Algorithmus steckt und ein entsprechendes Ergebnispapier dazu veröffentlicht hat, begründet dies damit, dass es eine „bittere Wahrheit" des Arbeitsmarktes sei, die sich im Arbeitsmarktmodell wi-

derspiegle. Laut AMS-Vorstand Johannes Kopf soll das System so vorbereitet werden, dass es den BeraterInnen sowie den KundInnen „die wichtigsten Gründe für die Einschätzung der Arbeitsmarktchancen" ausweist, um die Entscheidung nachvollziehen und gegen sie rechtlich vorgehen zu können.

Kritik

Angelika Adensamer, Juristin der Grundrechtsorganisation epicenter.works, warnt: „Es ist enorm wichtig, dass die Debatte über algorithmengestützte Entscheidungen möglichst breit geführt wird. Vor allem, wenn es um richtungsweisende Entscheidungen für das Leben von Menschen geht, ist besondere Vorsicht geboten. Die Gefahr, dass es dabei zu Diskriminierung und Fehlentscheidungen kommt, ist systemimmanent." Derzeit liege die Fehlerrate des Systems bei rund 50.000 Menschen pro Jahr, die falsch eingeordnet würden. Sie verweist auf die Betroffenenrechte: „Man hat das Recht, dass eine Entscheidung nicht ausschließlich vom Computer getroffen wird, sondern von einer echten Person." Dies sei gemäß der Darstellung von AMS-Vorstand Kopf hier der Fall. „Trotzdem steht zu befürchten, dass sich Beraterinnen und Berater auf die Ergebnisse verlassen, die von der Software vorgeschlagen werden."

Auch Experten der Universitäten TU und WU in Wien prognostizieren, dass viele AMS-SachbearbeiterInnen die Computer-Entscheidung einfach übernehmen werden und nicht hinterfragen. Diverse Studien belegten, dass das Ergebnis eines Computerprogramms die Entscheidung praktisch in jedem Fall mit beeinflusst. Dies wird von Adensamer ebenso gesehen: „Die Betroffenen und auch die Menschen, die auf Basis automatisierter Entscheidungen arbeiten, können nicht nachvollziehen, wie der Algorithmus funktioniert. Je komplexer er wird, desto mehr wird er zur Black Box. Das AMS ruft hier Geister, die im schlimmsten Fall die Zukunft von Menschen zerstören und die unsere Gesellschaft nur schwer wieder los wird." Die Datenschutzgrundverordnung (DSGVO) verbiete automatische Entscheidungen, die eine „nachteilige Rechtsfolge für betroffene Personen hat".

Die Entscheidung des Computerprogramms basiert auf in einem Data-Warehouse (DWH) gesammelten Daten. Es erfolgt eine Zusammenführung von statistischen Angaben mit Daten darüber, wie oft und wie lang jemand arbeitslos war, welchen Beruf er erlernt hat und welcher ausgeübt wurde. Wagner-Pinter erklärt: „Das DWH wird vom AMS im Rahmen rechtlich normierter Bedingungen geführt."

Rechtliche Grundlagen

Für Andreas Krisch, Geschäftsführer der Datenschutzagentur, handelt es sich hier um klassisches „Profiling": „Entsprechend notwendig ist es seitens des AMS, die Funktionsweise zu erläutern. Kunden haben ein Recht auf die Richtigstellung der Daten. Dazu muss man aber erst einmal rausfinden können, was eigentlich falsch ist. Man muss Gegenmaßnahmen setzen können. Für jeden Einzelnen hängt eine ganz wesentliche Entscheidung dran, ob man eine Schulung kriegt oder nicht." Adensamer bekräftigt: „Man hat ein Recht, die Daten, die einen betreffen, berichtigen zu lassen, nach Artikel 16 DSGVO. Das kann zumindest helfen, wenn die Berechnung auf falschen Daten beruht." Zudem gibt es für Betroffene ein generelles Auskunftsrecht laut DSGVO. Für beides werden Formulare zur Verfügung gestellt. Das AMS muss laut DSGVO in „präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" über das neue Computerprogramm aufklären, wozu auch die „involvierte Logik sowie die Tragweite einer Verarbeitung für die Person" gehört.

In Österreich gibt es ein „Gleichbehandlungsgesetz", in dem geregelt ist: „Auf Grund des Geschlechts, insbesondere unter Bezugnahme auf den Familienstand oder den Umstand, ob jemand Kinder hat, darf im Zusammenhang mit einem Arbeitsverhältnis niemand unmittelbar oder mittelbar diskriminiert werden." Es stellt sich die Frage, ob das Programm diese Vorgaben bei der Zulassung von Schulungsmaßnahmen beachtet wird. Betroffene können sich insofern an die Gleichbehandlungsanwaltschaft wenden. Diese wollte auf Presseanfrage jedoch keine Stellungnahme zur Frage abgeben, ob sie künftig auch Fälle von Diskriminierung durch den AMS-Algorithmus behandeln wird. Wirtschaftsinformatiker Krisch erklärt: „Amazon hat seinen Job-Algorithmus etwa eingestellt, weil es das Problem mit der Frauenfeindlichkeit nicht in den Griff bekommen hat. Wenn Amazon sein Programm zur Gänze einstellt wegen dieses Problems, ist dies ein Alarmsignal. Amazon hat hier deutlich mehr Erfahrung mit Algorithmen als das AMS." Hierauf angesprochen, erklärte AMS-Vorstand Kopf: „Bitte nicht vergessen, wir sind nicht Amazon oder irgendeine angeblich `böse´ Versicherung. Unser aller AMS ist jene Organisation, die seit ihrer Gründung täglich gegen Diskriminierung am Arbeitsmarkt kämpft und das auch weiter entschieden tun wird. Versprochen." Kopf wehrt sich gegen die Kritik mit dem Hinweis, dass die Chancenwert-Berechnung nur zeige, dass es auf dem Arbeitsmarkt eine Diskriminierung bestimmter Gruppen gebe. Ignoriere man diese Tatsache, so könnte nicht korrekt gefördert werden: „Unsere Aufgabe ist es, gegen Diskriminierung am Arbeitsmarkt vorzugehen." Der AMS sei z. B. verpflichtet, 50% seines Geldes für Fördermaßnahmen für Frauen auszugeben, obwohl 2017 nur 43,3% der Arbeitssuchenden weiblich gewesen seien. Für andere Gruppen, etwa Langzeitarbeitslose, gebe es ebenfalls spezielle Programme. Es sei deshalb nötig, dass der Algorithmus realistische Chancenwerte errechne: „Die Abbildung der Realität kann nicht diskriminierend sein."

Carla Hustedt, Leiterin des Projektes Algorithmen-Ethik der Bertelsmann-Stiftung sieht dies anders. Es könne wohl ein Problem sein, aus vorhandenen Datensätzen auf bestimmte Zusammenhänge zu schließen, „weil man damit womöglich bestehende Vorurteile reproduziert. Das muss einem bewusst sein und mit entsprechenden Maßnahmen verhindert werden." Sie meint, das Problem sei nicht die Software: „Hier wird dem Algorithmus die Schuld in die Schuhe geschoben. Eigentlich geht es um die Frage, welche Menschen in einem Solidarsystem die größte Unterstützung erhalten sollen." Das müsse politisch geklärt werden. Wichtig seien die Zwischentöne, um die konkreten Auswirkungen diskutieren zu können. Kopf vom AMS verspricht, auf diese Zwischentöne achten zu wollen. Der Einsatz der Software soll regelmäßig

überprüft und angepasst werden, und zwar auf mehreren Ebenen. Dazu zählt die Trefferquote und der Erfolg der eingesetzten Maßnahmen, aber auch, wie die Menschen in der Beratung mit dem Algorithmus umgehen: „Wir werden laufend überprüfen, ob unsere Berater dem Chancenwert in der Praxis eine zu hohe Bedeutung beimessen."

Und in Deutschland?

Gemäß einem Sprecher der deutschen Bundesanstalt für Arbeit (BA), die dem AMS entspricht, werden von der BA solche Algorithmen nicht genutzt. „Das ist derzeit auch nicht geplant." Bei der Beratung von Arbeitssuchenden wird eine Art Jobplattform genutzt, die Stellenangebote und Bewerberprofil vergleicht und dann passende Jobs vorschlägt. Dabei seien Qualifikation und Erfahrung wichtig, das Geschlecht und die Herkunft spielten dagegen keine Rolle (Wie ihr euch gegen den AMS-Algorithmus wehren könnt, Dornis, Arbeit vom Automaten, SZ 22.10.2018, 20; futurezone.at/netzpolitik/wie-ihr-euch-gegen-den-ams-algorithmus-wehren-koennt/400149528, 12-18.10.2018).

Schweiz

Referendum gegen Sozialschnüffelei

Ein Referendumskomitee hat 55.861 Unterschriften am 05.07.2018 bei der Bundeskanzlei in Bern gegen das Gesetz zur Überwachung von Sozialversicherten eingereicht, so dass hierüber voraussichtlich das Schweizer Stimmvolk zu befinden hat.

Knapp 75.500 Personen haben gemäß den Organisatoren das Referendum unterzeichnet; rund 20.000 Unterschriften seien aber zu spät eingetroffen, so dass sie von den Gemeinden nicht mehr überprüft werden konnten. Nötig für ein Referendum sind 50.000 beglaubigte Unterschriften. Das Referendum war unter anderem von den Sozialdemokraten (SP), den Grünen, dem Dachverband der Arbeitnehmenden Travail.Suisse sowie von Behinderten- und Seniorenorganisationen unterstützt worden.

Lanciert wurde das Referendum im April 2018 von einer Bürgerinnen- und Bürgergruppierung um die Autorin Sibylle Berg. Das von den eidgenössischen Räten im beschleunigten Verfahren bewilligte Gesetz stelle, so die Gruppierung, die Bevölkerung unter Generalverdacht, und die Privatsphäre der Menschen werde aufs Gröbste verletzt. Die Räte verabschiedeten das Gesetz in der Frühjahrssession. Es ermöglicht Sozialversicherungen, Versicherte bei Verdacht auf Missbrauch durch Detektive observieren zu lassen. Die Regeln gelten nicht nur für die Invalidenversicherung (IV), sondern auch für die Unfall-, die Kranken- und die Arbeitslosenversicherung. Neben Bild- und Tonaufnahmen sind auch technische Instrumente zur Standortbestimmung erlaubt. Gemeint sind vor allem GPS-Tracker, die an Autos angebracht werden. Anders als bei den Bild- und Tonaufnahmen braucht es dafür eine richterliche Genehmigung.

Angefangen hatte alles mit einem Luxus-BMW, der bei Protesten in Zürich am 1. Mai 2009 angezündet worden war. Dieses vermeintliche Symbol des Turbokapitalismus gehörte keinem Banker, keinem hochbezahlten CEO und keinem reichen mittelständischen Unternehmer aus dem Umland, sondern einer Sozialhilfeempfängerin. Der Fall machte Furore und inspirierte die Politik. Sozialmissbrauch, eines der Themen, das die rechte Schweizerische Volkspartei (SVP) seit Jahren auf der Agenda hatte, wurde zur Chefsache. Zürich wählte drastische Mittel; wenige Monate später nahmen sogenannte Sozialdetektive ihre Arbeit auf. Seit 2007 spionierten sie Menschen hinterher, die im Verdacht stehen, zu Unrecht Sozialleistungen zu beziehen.

Die rechtliche Grundlage für diese Observationen war dünn. Eine Schweizerin, die bei dem Europäischen Gerichtshof für Menschenrechte (EGMR) gegen die Praxis einer Unfallversicherung klagte, bekam in einem Urteil vom 18.10.2016 Recht (Nr. 61838/10 Vukato-Bojic/Schweiz). Die Richter monierten, dass es unklar sei, wie sich solche Eingriffe in die Privatsphäre mit dem Gesetz vereinbaren ließen. Besonders der Einsatz von GPS-Sendern, die Detektive zum Teil heimlich an Autos angebracht hatten, stand infrage. Zürich stellte die Beobachtungen ein.

Mitte März 2018 verabschiedete der Berner Nationalrat dann das Gesetz, das es den Sozialversicherungen schon bei geringem Verdacht erlaubt, Videos, Tonaufnahmen und Bewegungsprofile von Verdächtigen anzufertigen, was ein Freifahrtschein für Detektive ist. Dem Gesetz folgte ein Aufschrei, ganz ähnlich wie damals, als der BMW brannte. Innerhalb kürzester Zeit fand sich die Gruppe zusammen, die das Referendum gegen das Gesetz organisierte. Eines der besten Argumente gegen die Sozialdetektive bezog sich auf die Steuerpolitik der Schweiz. Denn während das Land bei SozialbetrügerInnen Härte zeigt, geht man mit SteuerbetrügerInnen seit jeher auffällig milde um. Hier gilt als heilig, was bei Arbeitslosen und anderen Bedürftigen als sekundär eingestuft wird: der Schutz der Privatsphäre (Unterschriften für Referendum gegen Sozialdetektive eingereicht, www.nzz.ch 05.07.2018; Theile, Zürcher Geschnüffeltes, SZ 16.04.2018 1)

Italien

DSGVO-Übergangsfrist für Kleinbetriebe

Der italienische Gesetzgeber hat mit einem im Amtsblatt der Republik veröffentlichten Anpassungsdekret auf Forderungen u. a. aus der Handwerkerschaft reagiert, wonach Betrieben eine Übergangsfrist von acht Monaten eingeräumt wird, sich an die neue Gesetzgebung der EU-Datenschutz-Grundverordnung (DSGVO) anzupassen. Die italienische Datenschutzbehörde wird in dieser Zeit weitere Leitlinien ausarbeiten, die vor allem zum Vorteil der Klein- und mittelständischen Betriebe sein und Vereinfachungen bringen sollen.

Der Präsident des südtiroler Landesverbands der Handwerker (lhv) Gert Lanz zeigte sich hierüber zufrieden: „Gemeinsam mit dem nationalen Handwerkerverband Confartigianato haben wir uns für eine Übergangsfrist stark gemacht. Die neue Regelung ist äußerst komplex und in vielen Fällen interpretationsoffen. Ziel unserer For-

derung war es, Kleinbetrieben eine Art Überbrückungszeit zu ermöglichen. Dies bedeutet allerdings nicht, dass das Thema Datenschutz für die Betriebe nun aufgeschoben oder aufgehoben ist. Im Gegenteil: Die Unternehmen haben nun genügend Zeit, sich über die neuen Bestimmungen und entsprechenden Umsetzungen in ihrer Firma zu informieren" (www.stol.it 28.08.2018, Datenschutz: Kleinbetrieben Übergangsfrist eingeräumt).

Portugal

400.000€-DSGVO-Bußgeld gegen Krankenhaus

In Portugal wurde die europaweit erste substanzielle Geldstrafe wegen eines Verstoßes gegen die neue EU-Datenschutz-Grundverordnung (DSGVO) verhängt. Die Datenschutzbehörde CNPD (Comissão Nacional de Protecção de Dados) gab am 22.10.2018 bekannt, dass das Krankenhaus Barreiro Montijo 400.000 € bezahlen soll. Der Großteil davon ist die Strafe dafür, dass viel zu viele Personen Zugriff auf Patientendaten hatten. Für einen anderen Verstoß wurden 100.000 Euro Strafe verhängt.

Der Krankenhausbetreiber hat laut Datenschutzaufsicht „bewusst" dafür gesorgt, dass Nutzende mit dem Profil „Techniker" in den IT-Systemen auf Daten zugreifen konnten, die eigentlich nur für Ärzte einsehbar sein dürfen. Das sei bei einem Test ermittelt worden, in dessen Rahmen solch ein Profil mit unbegrenztem Zugang erstellt werden konnte. Darüber hinaus seien in dem System insgesamt 985 aktive Benutzende mit einem Profil „Arzt" registriert, obwohl 2018 lediglich 296 Ärzte eingeteilt worden seien. Das Krankenhaus habe die Diskrepanz mit temporären Profilen im Rahmen eines Dienstleistungsvertrags zu erklären versucht. Das Krankenhaus Barreiro Montijo hatte im Juli 2018 Besuch von den Datenschützern erhalten. Deren Schlussfolgerungen teilt es nicht, das Krankenhaus will deswegen vor Gericht gehen (Holland, DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen, www.heise.de 23.10.2018).

Tschechien

Beschwerdeflut bei Datenschutzbehörde

Das staatliche Amt für Datenschutz in Tschechien (ÚOOÚ) versinkt gemäß eigenen Angaben vom Juli 2018 in Beschwerden. Im ersten Halbjahr dieses Jahres sind rund 630 Anträge bei der Behörde eingegangen, was in etwa das Dreifache im Vergleich zum Vorjahreszeitraum sei. Der Anstieg bei den Beschwerden liege an der neuen europäischen Datenschutz-Grundverordnung (DSGVO), die seit Mai auch in Tschechien in Kraft ist. Die meisten Antragstellenden würden sich an ungefragten Kameraaufnahmen oder ungebetenen Werbeanrufen stören (Bucan, Beschwerden beim Datenschutz-Amt auf Rekordniveau, www.radio.cz 15.07.2018).

Großbritannien

Bußgeld gegen Facebook wegen Cambridge Analytica

Die britische Datenschutzbehörde Information Commissioner's Office (ICO) hat gemäß einer Information vom 25.10.2018 gegen Facebook die bisher maximale Strafe in Höhe von 500.000 Pfund (565.000 €) wegen des Datenskandals um Cambridge Analytica bestätigt. Das Unternehmen habe einen „schweren Verstoß" gegen geltendes Recht zugelassen. Repräsentanten des Konzerns hätten keine hinreichenden Gegenargumente vorgebracht. Weltweit waren nach Berechnungen des ICO ca. 87 Mio. Menschen von dem Datenskandal betroffen. Die britische Datenschutz-Kommissarin Elizabeth Denham erklärte: „Facebook hat es versäumt, die Privatsphäre seiner Nutzer vor, während und nach der rechtswidrigen Verarbeitung dieser Daten ausreichend zu schützen. Ein Unternehmen dieser Größe und mit dieser Expertise hätte es besser wissen und es besser machen sollen."

Bei dem Datenskandal hatte der Entwickler einer Umfrage-App vor mehr als vier Jahren Informationen von Facebook-Nutzern unrechtmäßig an die Firma Cambridge Analytica weitergereicht, die später unter anderem für das Wahlkampfteam von US-Präsident Donald Trump arbeitete. Dabei ging es nicht nur um die Daten der rund 300.000 Umfrage-Teilnehmenden, sondern auch um die ihrer Facebook-Freunde. Der Daten-Zugriff für App-Entwickler ließ diesen breiten Einzug von Informationen von 2007 bis 2014 zu. Cambridge Analytica hat inzwischen den Geschäftsbetrieb eingestellt.

Das ICO bemängelte nun, dass Facebook den App-Entwicklern ohne eine rechtliche Basis Zugang zu den Daten gewährt habe: „Zwischen 2007 und 2014 hat Facebook die personenbezogenen Daten von Nutzern unrechtmäßig verarbeitet, indem es Anwendungsentwicklern ohne hinreichend klare und informierte Zustimmung Zugang zu ihren Daten gewährt hat. Der Zugang wurde auch dann ermöglicht, wenn die Nutzer die App nicht heruntergeladen haben, sondern einfach nur mit Personen befreundet waren, die die App hatten."

In Deutschland wurde Facebook wegen des Vorgangs nicht belangt. Anfang Oktober 2018 stellte der Hamburger Datenschutzbeauftragte Johannes Caspar sein Bußgeldverfahren gegen Facebook in dieser Sache ein. Zur britischen Entscheidung erklärte ein Facebook-Sprecher nun, sein Unternehmen prüfe derzeit die Entscheidung des ICO. Bei allem Respekt sei Facebook mit manchen Ergebnissen der Untersuchung nicht einverstanden. Gleichwohl habe man selbst zuvor gesagt, dass Facebook mehr hätten tun sollen, um die Behauptungen über Cambridge Analytica zu untersuchen (500.000 Pfund: Britische Datenschützer bestätigen Höchststrafe gegen Facebook, www.heise.de 25.10.2018).

Großbritannien

Kreditkartenklau bei British Airways

Bei Buchungen über die Internetseite und die App von British Airways sind nach Angaben der Fluggesellschaft die Daten von etwa 380.000 Kreditkarten gestohlen worden. Betroffen seien persönliche und finanzielle Details, nicht aber Pass- und Reisedaten. Demnach konnten die Informationen über einen Zeitraum von rund zwei Wochen – vom

Abend des 21.08.2018 bis zum Abend des 05.09.2018 – abgegriffen werden. Man sei in Kontakt mit betroffenen KundInnen, heißt es von British Airways. Die Behörden seien informiert worden (Daten von 380 000 Kreditkarten weg, Kieler Nachrichten 08.09.2018, 7).

Schweden/USA

Spotify kooperiert mit Genanalysefirma Ancestry

Der schwedische Milliardenkonzern Spotify hat sich mit dem Genanalyse-Unternehmen Ancestry zusammengetan: Wer will, schickt eine Speichelprobe an Ancestry, wo Forschende aus der DNA-Probe die Herkunft der Ahnen entschlüsseln. Anschließend bekommt man Lieder von Spotify aus jenen Ländern präsentiert, in denen man angeblich seine Wurzeln hat. Die Genauigkeit dieser Tests ist sehr umstritten. So hatte z. B. eine Amerikanerin eine italienische Oma, die ihr aber vom Gentest abgesprochen wurde. Als Mensch mit deutscher Herkunft muss man bei diesem einseitigen Tauschgeschäft besonders aufpassen. Es kann passieren, dass man sensibelste Informationen gegen eine Liedempfehlung für „Revolverheld" oder den Schlagersänger Wolfgang Lippert eintauscht. Beide haben es in die DNA-Playlist für Deutschland geschafft.

Spotify hat erkannt, dass beim einst so heiklen Thema DNA-Test inzwischen für viele fast alle Hemmungen über Bord gegangen sind. 15 Millionen Menschen haben bereits ihr Erbgut von privaten Firmen entschlüsseln lassen, als wäre dies das Normalste auf der Welt. Manchen geht es dabei um ernste Anliegen, wie das Risiko für Brustkrebs zu identifizieren oder die Wirksamkeit von Medikamenten zu bestimmen. Andere treibt allein der narzisstische Wille an, ein bisschen mehr über sich selbst zu erfahren, zum Beispiel, weil das angeblich bei der Partnerwahl helfen könnte.

Niemand sollte sich wundern, dass die Daten von den Genanalyse-Firmen weitergereicht werden, insbesondere an Pharmakonzerne. Dass die Daten anonymisiert seien, ist nur oberflächlich korrekt. WissenschaftlerInnen haben schon 2013 im Fachmagazin „Science" nachgewiesen, dass ein Mann nur durch die Abfolge seiner Y-Chromosomen und den Abgleich in einer öffentlichen Datenbank identifiziert werden konnte. Die Geschäftsbedingungen können sich jederzeit ändern, im Fall eines Hacks wollen die Firmen keine Verantwortung übernehmen. In Amerika haben sich die Gesundheitsbehörden deshalb einen ganz praktischen Rat überlegt: „Think before you spit." Bedeutet: Schalte dein Gehirn ein, bevor du deinen Speichel an eine Firma schickst (Geschwendtner, Erst denken, dann spucken, SZ 29./30.09.2018, 33).

Russland

Staatliche Prämien für „Informanten"

Das russische Innenministerium bietet seit Ende August 2018 BürgerInnen Prämien von umgerechnet 640 € bis zu 128.000 € für Informationen über Verbrecher an, wenn die Polizei um Hinweise aus der Bevölkerung bittet. Die Anzeigen werden auf der offiziellen Webseite des Ministeriums veröffentlicht. Belohnt wird, wenn sich die Hinweise als richtig erweisen und der Täter gefasst werden kann. Anonymen Tipps geht die Polizei nach eigenen Angaben nicht nach. Die „Informanten", wie die russischen Behörden diese Personen nennen, müssen mit Klarnamen auftreten.

Ziel des russischen Innenministeriums ist es, so das russische Internetportal Mediazona, das sich mit dem Strafvollzugs- und Justizwesen beschäftigt, die Aufklärungsquote von Straftaten zu verbessern. Russische MenschenrechtlerInnen sehen in dem neuen Gesetz aber auch eine Gefahr für die Gesellschaft: Mehr als 20 Millionen RussInnen leben laut einer Statistik der Rechnungskammer in Armut. Nach Informationen von Wziom, einem russischen Meinungsforschungszentrum, hat mehr als die Hälfte der Bevölkerung keine Ersparnisse. Der finanzielle Anreiz, Hinweise an die Polizei zu liefern, könnte also bei vielen Menschen so hoch sein, dass es zu wahllosen Denunziationen kommt.

Bislang ist nicht festgelegt, wen die Polizei mit Hilfe der BürgerInnen dingfest machen möchte, Räuber und Mörder – oder auch Menschen, die regierungskritische Meinungen im Internet vertreten. Gemäß offiziellen Angaben der Generalstaatsanwaltschaft saßen 2017 mehr als 1.500 Menschen wegen ihrer Aktivitäten in sozialen Netzwerken im Gefängnis. Für eine Haftstrafe genügt es, regierungskritische Bilder zu speichern, andere zu zitieren oder einen Post zu schreiben. Im Fokus stehen dabei vor allem Oppositionelle, aber auch AtheistInnen und FeministInnen. Während der Zeit der Sowjetunion waren Denunziationen an der Tagesordnung. Opfer berichten bereits über Fälle von Erpressung im Internet. Zum Beispiel werden sie, so Medienberichte, darauf aufmerksam gemacht, dass sich verbotene Bilder oder Posts auf ihrem Social-Media-Kanal befinden. Ihnen wird gedroht, sie bei der Polizei zu verraten, wenn sie nicht bezahlen oder Nacktfotos von sich zur Verfügung stellen.

Albert Ptschelinzew, Menschenrechtler und Präsident der überregionalen Bürgerorganisation „Gegen die Korruption", erklärte: „Einige Leute wollen jemandem schaden und auf diese Weise auch noch Geld verdienen." Er meint aber auch, dass das Risiko des Gesetzes, die Korruption von Polizisten zu fördern, minimal sei. Denis Michailow, der Leiter der Organisation von Alexej Nawalny in Sankt Petersburg, erklärte dagegen, dass die Korruption durch das neue Gesetz zunehmen wird: „Die Leute, die mit der Polizei gutgestellt sind, können auch Informanten sein." Er erinnert an Maria Motuznaja, eine 23-jährige Studentin aus Barnaul, der eine Haftstrafe von bis zu sechs Jahren droht. Sie wurde von zwei Praktikantinnen aus dem Innenministerium beschuldigt, sich im sozialen Netzwerk VKontakte, dem russischen Äquivalent von Facebook, beleidigend über Schwarze und Religiöse geäußert zu haben. Sie soll diskriminierende Illustrationen von Priestern und Schwarzen geteilt haben und ist vor Gericht wegen „Beleidigung der Gefühle von Gläubigen" angeklagt. Michailow vermutet hinter dem neuen Gesetz vor allem eine Methode für die Jagd auf Oppositionel-

le: „Wenn das Gesetz dabei hilft, Räuber oder Mörder zu verhaften, dann ist das gut. Aber in Russland wird es als Methode der politischen Druckausübung auf die Opposition benutzt“ (Sauer, Nebenjob Denunziant, SZ 05.09.2018, 9).

Kanada

Abschiebung dank DNA-Familienforschung

Die Canada Border Services Agency (CBSA), die kanadische Ausländerbehörde, sammelt DNA von Flüchtlingen, um diese mit Familienforschungs-Gendatenbanken abzugleichen und so entfernte Verwandte sowie die Staatsangehörigkeit zu bestimmen. Subodh Bharati, Rechtsanwalt eines Mannes, der behauptet aus Libyen zu kommen und dem die Behörden dessen nigerianische Staatsangehörigkeit nachweisen wollen, erklärte: „Ich denke, es ist von öffentlichem Interesse, dass Grenzbehörden wie die CBSA den Zugang zu Gendatenbanken wie Familytreedna.com und Ancestry.com nutzen, um Gendatenabgleiche durchzuführen. Hiergegen bestehen Datenschutzbedenken: Wie ist es CBSA möglich, an diese Informationen zu kommen und durch welche Maßnahmen wird gewährleistet, dass diese Informationen vertraulich bleiben?“ Bharati vertritt seinen Mandanten im Auftrag von CLASP, eine juristische Hilfsorganisation der Osgoode Hall Law School. Er erklärte, ihm seien zwei Personen bekannt, die Familytreedna.com nutzten, einer davon aus Großbritannien, die von der CBSA kontaktiert wurden mit dem Ziel der Erlangung von Informationen, mit denen eine Abschiebung aus Kanada ermöglicht wird. „Personen, die diese Angebote nutzen, um ihren Familienstammbaum zu recherchieren, sollten sich darüber bewusst sein, dass ihre vertraulichen Informationen Regierungsstellen verfügbar gemacht werden, und dass Grenzbeamte möglicherweise Kontakt mit ihnen aufnehmen, um die Abschiebung von Migranten zu ermöglichen“ (Khandaker, Canada is using ancestry DNA websites to help deport people, news.vice.com 26.07.2018).

USA/weltweit

Google gewährt Entwicklern Zugriff auf E-Mail-Inhalte

Google teilte mit, dass es weiterhin anderen Firmen Zugriff auf E-Mails seiner Nutzenden gewähren wird. Googles Vorgehen wird von Datenschützern kritisiert, seit Google sein Mail-Programm Gmail 2004 anbietet. Damals glaubten zunächst viele an einen Scherz, denn Google versprach jedem Nutzer so viel Speicherplatz, dass er nie mehr eine E-Mail würde löschen müssen. Die Begeisterung wich bald Besorgnis um die Vertraulichkeit, als sich herausstellte, dass Google diesen für die Nutzenden kostenlosen Service mit Werbung finanziert, die jeder anderen an Treffsicherheit überlegen war. Denn Googles Software analysierte die Mails seiner Nutzenden, um ihnen passgenaue Werbung anzeigen zu können. Wer also in seinen Mails von Plänen erzählte, Paris zu besuchen, der bekam möglicherweise bald Werbung für Pariser Hotels zu sehen.

Google konnte noch so oft erklären, dass keineswegs Mitarbeitende die Mails lesen, sondern dass lediglich Software-Programme die Nachrichten analysierten. Das Misstrauen blieb. Im vergangenen Jahr dann gab Google die Erklärungsversuche auf und verkündete, man höre auf, Mail-Inhalte zu scannen. Damit wollte das Unternehmen den KundInnen versichern, dass ihre Daten geschützt seien. Mitarbeitende erhielten nur in seltenen Fällen Zugang zu den Nachrichten, etwa bei der Untersuchung von Sicherheitszwischenfällen oder zur Fehlersuche; dann frage Google die Nutzenden aber gesondert um Erlaubnis. Eine Auswertung für Werbezwecke erfolge definitiv nicht (mehr).

Wohl kaum einE NutzerIn rechnete damit, dass diese Erklärung nicht ausschloss, dass Google anderen Unternehmen dieses Recht einräumen könnte. Gemäß einem Pressebericht vom Sommer 2018 haben zahlreiche Entwickler von Apps Zugriff auf die Mail-Inhalte von Gmail-Nutzenden. Dabei geht es zum Beispiel um Apps, die helfen, Mails zu sortieren oder Reisepläne auszuarbeiten. Zwar müssen Nutzende diesen Programmen ausdrücklich den Zugriff gewähren. Das geschieht in der Regel für die Nutzung von kostenlosen Mail-Diensten wie automatischen Reiseplanern oder Preisvergleichs-Portalen. In dem Pressebericht wird unter anderem die Firma Return Path genannt, die auf diese Weise bis zu 100 Millionen E-Mails pro Tag analysieren soll. Auch alternative Gmail-Clients sichern sich Leserechte für das E-Mail-Konto der Anwendenden. Der Firmenchef des Entwicklungsstudios hinter der Mail-App Edison gab zu, dass seine Entwickler die Mails Hunderter Nutzender seines Gmail-Clients gelesen haben. Diese Praxis sei unter App-Entwicklern völlig normal und sei durch die AGB der jeweiligen Apps oder Dienste abgedeckt.

Es war bisher unklar, in welchem Ausmaß die App-Entwickler die Nachrichten auch analysierten. Manche der Drittfirmen werten die Nachrichten vollautomatisch aus, andere lassen ihre Mitarbeitende von Hand in E-Mails schauen, etwa um die eigene Software zu trainieren. In einigen Tausend Fällen hatten Entwickler gemäß den Berichten Mails tatsächlich gelesen, um ihre Programme noch zielgenauer zu machen. In dem Bericht bezeichnet der Cheftechniker einer der beteiligten Unternehmen das Vorgehen als „üblich“ und als „schmutziges Geheimnis“ der Branche.

Dies veranlasste einige US-Senatoren, Google schriftlich zur Stellungnahme aufzufordern. In einem Brief schrieb der Konzern nun, er gewähre Entwicklern weiterhin Zugriff auf persönliche Mails seiner Nutzenden und räume ihnen sogar das Recht ein, die Inhalte mit anderen zu teilen. Das alles geschehe aber nur, wenn sichergestellt sein, dass die Nutzenden darüber aufgeklärt würden, was mit ihren Daten geschehe. Darüber hinaus prüfe man regelmäßig den Umgang der App-Entwickler mit den Inhalten der Nutzenden. Google geht in seiner Stellungnahme nicht auf die Rechte jener ein, die zwar mit Gmail-Nutzenden Mails austauschen, die aber niemals einer Analyse ihrer Nachrichten zugestimmt haben, weil sie selbst gar keine Google-KundInnen sind.

Für Firmen, die an Kundendaten interessiert sind, gibt es kaum einen größeren Schatz als die Nachrichten der 1,4 Milliarden Gmail-Nutzenden. Sie be-

inhalten wertvolle Informationen über Kaufverhalten, Reisepläne, Finanzen und persönliche Vorlieben. Um an diese Informationen zu gelangen, bieten solche Firmen gerne kostenlose Apps an, in deren Nutzungsbedingungen Zugriff auf die Mails verlangt wird (Conradi, Suchen, finden, lesen, SZ 24.09.2018, 19; Nickel, Datenschutz: Drittfirmen lesen massenweise Gmail-Postfächer, www.golem.de 03.07.2018).

USA

Aufgekaufte Gründer verlassen Facebook

Anfang August 2018 kündigte Whatsapp an, erstmals Werbung schalten zu wollen. Damit gab das von Facebook 2014 für etwa 22 Mrd. Dollar aufgekaufte Unternehmen ein Grundprinzip dieses Angebots, dem sich dessen Gründer verpflichtet sahen, auf. Die App sollte, so der Whatsapp-Gründer Brian Acton, frei von Werbung bleiben. Doch die Chefs von Facebook, Mark Zuckerberg und Sheryl Sandberg, wollten endlich Geld mit Whatsapp verdienen. Deshalb verließ der heute 46-jährige Acton Facebook 2017 und verzichtete durch seinen abrupten Abgang auf 850 Mio. Dollar, die ihm zugestanden hätten, wenn er länger bei Facebook geblieben wäre. Acton beschrieb nun gegenüber dem Magazin Forbes, wie Whatsapps Kultur des Respekts gegenüber den Nutzenden mit Facebooks Profitmaxime kollidierte. In Facebooks Führungsriege seien „gute Geschäftsleute. Sie stehen nur für eine Reihe von Geschäftspraktiken, Prinzipien und Ethik, mit denen ich nicht unbedingt einverstanden bin." Die Whatsapp-Gründer Acton und Jan Koum wurden mehrfache Milliardäre. Dem ehemaligen Yahoo-Ingenieur Acton hatten 20% an Whatsapp gehört. Er verließ als erster Facebook; Koum folgte ihm im Frühjahr 2018. Mitte September 2018 gingen auch die Gründer von Instagram, Kevin Krieger und Kevin Systrom. Facebook hatte Instagram 2012 für weniger als eine Milliarde Dollar gekauft, als es 30 Millionen Nutzende hatte. Inzwischen wird Instagram von über einer Milliarde Menschen genutzt.

Acton berichtet, dass bei Whatsapp in Ruhe und überlegt gearbeitet worden war; Facebook habe dagegen nach seinem Motto „Move fast und break things" gehandelt. Die Whatsapp-Gründer hätten mit Zuckerberg vereinbart, dass es fünf Jahre lang „null Druck" geben solle, Geld zu verdienen. Doch habe Facebook schon bald darauf hingearbeitet, Werbung in der App zu platzieren. Dagegen hatten Acton und Koum den Nutzenden die Achtung des Datenschutzes versprochen, so Acton: „Ich habe die Privatsphäre meiner Nutzer für einen größeren Nutzen verkauft. Ich habe eine Wahl getroffen und einen Kompromiss gemacht. Und ich lebe jeden Tag damit." Das Geschäftsmodell Whatsapp sollte nach den Vorstellungen von Acton mit Minibeträgen finanziert werden, die die Nutzenden zahlen. Doch das widersprach dem Plan Sandbergs, die meinte: „Das skaliert nicht." Skalierbarkeit ist ein Mantra für Geschäftsmodelle im Silicon Valley. Ebenso habe ihn der Datenaustausch zwischen Whatsapp und Facebook geärgert. Als die EU-Kommission die Übernahme seiner Firma durch Facebook prüfte, sei er „gecoacht" worden, um zu erklären, dass es technisch sehr schwierig sein, die Daten zu verschmelzen. Später habe er erfahren, dass Facebook genau daran arbeitete. Wenig später wurde die Verknüpfung der Nutzungsdaten verkündet. Acton ließ zudem durchblicken, wie unzufrieden er mit dem Krisenmanagement angesichts der Einflussnahme im US-Wahlkampf gewesen sei. Und im März 2018 twitterte Acton in Reaktion auf den Datenskandal mit Cambridge Analytica den Hashtag #deleteFacebook und forderte auf, der Plattform den Rücken zu kehren.

David Markus, bei Facebook für die Messenger-Apps zuständig, widersprach Acton: Whatsapp sei bemerkenswert viel Eigenständigkeit gewährt worden. Whatsapps Ende-zu-Ende-Verschlüsselung habe Zuckerberg nie in Frage gestellt, so wie Acton behauptet.

Mit dem Aufkauf von Whatsapp und Instagram hat sich Facebook ein Problem vom Hals gehalten: dass ihm die jungen Menschen den Rücken zukehren. Auch Krieger und Systorm hatten bis zum Ende darauf bestanden, dass das übernommene Instagram größtenteils unabhängig bleibt von Facebook. Weil Instagram für den Erfolg des Konzerns immer wichtiger wurde, hatte Zuckerberg vor dem Weggang der Gründer sich immer mehr eingemischt. Mit dem Abgang wird die Fotoplattform wohl noch enger an den Konzern gebunden.

Weitere langjährige Weggefährten Zuckerbergs verließen jüngst das Unternehmen. So ging auch Palmer Luckey, der Gründer des übernommenen Videobrillen-Herstellers Oculus Rift. Insgesamt hat Zuckerberg in den vergangenen 18 Monaten alle Gründer verloren, deren Unternehmen er eingekauft hatte. Auf die Frage nach seinem Idol, antwortete Zuckerberg „Augustus". Dieser römische Kaiser hatte sich nach dem Tod Julius Cäsars bei den Machtkämpfen um die Nachfolge durchgesetzt und die römische Republik in eine Monarchie umgekrempelt. Schon vor Jahren nannte er seine Firma das „Mark Zuckerberg-Produkt". Er scheint gewillt zu sein dafür zu sorgen, dass dies so bleibt (Brühl, Die Abrechnung, SZ 28.09.2018, 15; Warum laufen Facebook die Manager weg? Der Spiegel Nr. 40, 29.09.2018, 59; Conradi/Wischmeyer, Alleinherrscher, SZ 26.09.2018, 20).

USA

Google beschafft sich Kreditkartendaten von Mastercard

Google hat gemäß Medienberichten einen Weg gefunden, um Online-Anzeigen mit Offline-Einkäufen zu verknüpfen. Hierzu hat der IT-Konzern offenbar einen bislang geheimen Vertrag mit der Firma Mastercard abgeschlossen, die Transaktionsdaten von deren KundInnen an Google übermittelt. Die Verhandlungen dazu sollen vier Jahre gedauert haben. Der Bericht stammt vom Mediendienst Bloomberg, der sich bei der Geschichte auf vier anonyme Quellen, von denen drei direkt in den Deal involviert gewesen seien, beruft. Google soll für die Transaktionsdaten mehrere Millionen US-Dollar bezahlt haben.

Ausgewählte Firmen, die bei Google Werbung schalten, hatten 2017 Zugriff auf ein Tool, das auf den Transaktionsdaten beruht. So sahen sie, ob Google-Nutzende das online beworbene Produkt später in einem Laden kauften. Das Tool bot Google, soweit bekannt, nur in den USA an. Dass diese Verbindung zustan-

de kam, wussten die KundInnen nicht, da die beiden Unternehmen nie darüber informiert haben.

Christine Bannan vom Electronic Privacy Information Center (EPIC) kritisiert die Datenweitergabe: „Die Menschen erwarten nicht, dass ihre Einkäufe in einem Laden mit ihrem Online-Shopping abgeglichen werden." Die Firmen würden ihre Pflichten nicht wahrnehmen, da sie die KundInnen nicht darüber informierten, was sie tun und welche Rechte die Kunden hätten. Eine Google-Sprecherin gab an, dass keine Informationen mit den Werbepartnern geteilt würden. Zudem könnten KundInnen das Tracking der Kreditkarte in den Konto-Einstellungen deaktivieren (Google weiß, was seine Nutzer im Laden kaufen, www.lessentiel.lu/de 03.09.2018).

USA

Computerirrtum bei Wells Fargo: Häuser verloren

In einem Bericht für das zweite Quartal 2018, den die US-Bank Wells Fargo bei der US-Börsenaufsicht SEC einreichte, erwähnt die Bank einen Softwarefehler in einem kurzen Abschnitt, wegen dem etwa 400 KundInnen der US-Bank von Jahr 2010 an ihre Häuser verloren haben. Dies hatte sich bei einer internen Überprüfung der Hauskredite ergeben. Fünf Jahre lang berechnete eine Software offenbar immer wieder falsche Beträge und Gebühren, als KundInnen in den USA versuchten, ihre Hauskredite anzupassen. Erst im Oktober 2015 wurde die Software so verändert, dass der Fehler nicht mehr auftrat. Bis dahin waren schon 625 Kunden betroffen. Bei etwa 400 von ihnen wurden die Kreditanpassungen nicht nur abgelehnt, sondern, so der Bericht, auf Basis der fehlerhaften Werte auch Zwangsvollstreckungen durchgeführt. Eine Sprecherin von Wells Fargo bestätigte, dass die KundInnen ihre Häuser verloren hätten. Die Bank entschuldige sich dafür. Wells Fargo stellte nach eigenen Angaben acht Millionen Dollar zurück, um die Betroffenen entschädigen zu können.

Wells Fargo, eine der größten Banken der USA, fiel schon mehrmals mit Datenskandalen auf: Im September 2016 kam heraus, dass Mitarbeitende teilweise mit Kundendaten Millionen gefälschte Bankkonten erstellt hatten, um damit die Zahlen zu schönen. Auch hier musste Wells Fargo eine Strafe zahlen, sie betrug 185 Millionen Dollar. Außerdem verloren nach Angaben der Bank Tausende Mitarbeitende ihren Job. Im vergangenen Jahr reichte Wells Fargo über eine Anwaltskanzlei in einem Gerichtsverfahren aus Versehen die vertraulichen Informationen von fast 50.000 vermögenden KundInnen weiter, inklusive Sozialversicherungsnummern, bezahlten Gebühren und Investment-Portfolios (Dornis, Wenn der Computer irrt, SZ 07.08.2018, 22).

Brasilien

Datenschutzgesetz nach DSGVO-Vorbild verabschiedet

Am 14.08.2018 wurde für Brasilien ein neues allgemeines Datenschutzrecht (Lei Geral de Proteção de Dados) verabschiedet. Das neue Gesetz führt, dem europäischen Recht der Datenschutz-Grundverordnung (DSGVO) folgend, flächendeckende Reglungen zum Schutz personenbezogener Daten sowohl für den öffentlichen als auch für den privaten Sektor, online wie offline, ein. Es werden Erlaubnistatbestände für die Datenverarbeitung geschaffen und Betroffenenrechte festgelegt. Neben den brasilianischen Unternehmen und Behörden wird das Gesetz auch für ausländische Unternehmen gelten, die mindestens eine Niederlassung in Brasilien haben oder Dienstleistungen für den brasilianischen Markt anbieten.

Personenbezogene Daten (dados pessoais) sind alle Daten, die isoliert oder im Zusammenhang mit anderen Daten, zur Identifizierung einer natürlichen Person führen können (Art. 5° inciso I). Dazu dürften auch pseudonymisierte Daten gezählt werden. Anonymisierte Daten, die unter Berücksichtigung der zum Zeitpunkt der Datenverarbeitung verfügbaren Zeit, Kosten und technischen Möglichkeiten nicht zu einer Identifizierung der Betroffenen herangezogen werden können, fallen nicht darunter.

Sensitive Daten (dado pessoal sensível) werden besonders geschützt werden. Nach Art. 5° inciso II handelt es sich dabei um solche über die rassische oder ethnische Herkunft, die religiöse Überzeugung, die politische Meinung, Gewerkschaftszugehörigkeit oder Zugehörigkeit zu einer Organisation mit religiösen Charakter, die Gesundheit, das Sexualleben, oder Daten die eine eindeutige und dauerhafte Identifizierung des Betroffenen ermöglichen, wie etwa genetische- oder biometrische Daten.

Es werden zehn Grundsätze (princípios gerais de proteção) in Art. 6° aufgestellt, die bei der Datenverarbeitung berücksichtigt werden sollen, u. a. Zweckbindung, Notwendigkeit, die Qualität der Daten, Transparenz, Sicherheit, Nichtdiskriminierung und das Prinzip der Rechenschaftspflicht, wonach der für die Verarbeitung Verantwortliche und der Datenverarbeiter wirksame Maßnahmen des Datenschutzes umfassend und transparent nachweisen können müssen. Dies kann durch Datenschutzüberprüfungen erfolgen, die auch gesetzlich geregelt sind.

Die Betroffenen haben das Recht auf Zugang zu den Daten, Berichtigung, Löschung oder Ausschluss, Widerspruch gegen die Behandlung und das Recht auf Information und Erklärung über die Verwendung der Daten (direitos do titular). Wie durch die DSGVO wird auch in Brasilien der Betroffene ein Recht auf Datenübertragbarkeit haben, welches ermöglicht, nicht nur eine Kopie der Daten anzufordern, sondern sie auch in einem systemkompatiblen Format zur Verfügung zu erhalten, das eine Übertragung der Daten auf andere Dienste, erleichtern soll.

Eine Übermittlung in andere Länder (transferência internacional de dados) wird ermöglicht, auch wenn dort kein angemessenes Schutzniveau besteht. Dies ist in Kapitel V des Gesetzes geregelt. Die Daten müssen dafür entweder auf Grundlage einer Einwilligung der Betroffenen übermittelt werden, oder der Verantwortliche muss durch verbindliche Unternehmensregeln und Standardklauseln garantieren, dass die Grundsätze des Datenschutzes eingehalten werden.

Das Gesetz lässt in Art. 41 den Schluss zu, dass künftig jede datenverarbeitende Stelle, einen Datenschutzbeauftragten (encarregado pelo tratamento de

dados pessoais) benennen muss. Allerdings kann die noch zu schaffende nationale Datenschutzbehörde ergänzende Voraussetzungen vorgeben, bei deren Vorliegen ein Unternehmen keinen DSB benennen muss.

Auch eine Art Folgenabschätzung (relatório de impacto à proteção de dados pessoais) wird für Datenverarbeitungstätigkeiten, die bestimmte Risiken für die betroffenen Personen mit sich bringen können, durchgeführt werden müssen. Dabei sind Maßnahmen und Schutzvorkehrungen zur Begrenzung der Risiken aufzuführen.

Des Weiteren sind auch Aufzeichnungen (relatório de impacto à proteção de dados pessoais) erforderlich, die an ein Verarbeitungsverzeichnis erinnern, denn es ist jeder Schritt der Datenverarbeitung, die Arten der Daten, die jeweilige Rechtsgrundlage, Zwecke, Speicherdauer und die Maßnahmen der Informationssicherheit, zu dokumentieren.

Verantwortliche und Datenverarbeiter haben zudem geeignete sicherheitstechnische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen. Die Datenschutzbehörde kann dazu technische Mindeststandards festlegen. Auch privacy by design und by default sollen in Brasilien gelten.

Die an der Datenverarbeitung Beteiligten werden gesamtschuldnerisch haften. Bei Verstößen können Sanktionen (Sançóes Administrativas) nach Art. 52 in Höhe von 2 Prozent des Unternehmensumsatzes des letzten Geschäftsjahres, begrenzt auf insgesamt fünfzig Millionen Reais (ca. 11,3 Millionen Euro) verhängt werden. Datenschutzverletzungen sind innerhalb eines angemessenen Zeitraumes an die Datenschutzbehörde zu melden, welche je nach Schwere des Falles die Meldung an alle betroffenen Personen oder auch an die breite Öffentlichkeit anordnen kann.

Die vom brasilianischen Gesetzgeber vorgesehenen Regelungen ähneln stark der europäischen DSGVO. Daraus lässt sich schließen, dass eine gegenseitige Anerkennung eines angemessenen Datenschutzniveaus durch die EU-Kommission und die zukünftig zuständige brasilianische Behörde, vorgesehen ist, um künftig den Datentransfer zwischen brasilianischen und EU-Unternehmen zu vereinfachen.

Das Gesetz wird ab Anfang 2020 unmittelbar anzuwenden sein. Es wird also wie bei der DSGVO eine Frist geben, die den brasilianischen Unternehmen Zeit gibt, ihre Prozesse datenschutzkonform zu gestalten und an das neue Recht anzupassen (Neuer brasilianischer Datenschutz, www.datenschutzbeauftragter-info.de 16.08.2018).

Japan

Olympische Spiele 2020 mit Gesichtserkennung

In Tokio werden 2020 die ersten Olympischen Spiele stattfinden, bei denen Gesichtserkennung an allen Veranstaltungsorten zum Einsatz kommt. Die Veranstalter haben am 07.08.2018 bekannt gegeben, dass eine Adaption der „NeoFace"-Technologie von NEC für „mehr Sicherheit" sorgen und den AthletInnen unnötigen Stress ersparen soll. An über 40 Veranstaltungsorten sind, so Tsuyoshi Iwashita, Sicherheitschef für Tokio 2020, Sicherheitschecks durchzuführen: „Die Veranstaltungsorte in Tokio haben nicht immer genug Platz für Sicherheitschecks und Warteschlangen". Die Gesichtserkennung soll zumindest für voraussichtlich über 300.000 akkreditierte Personen wie AthletInnen, BetreuerInnen, Offizielle und MedienvertreterInnen Abhilfe schaffen. Sie werden Fotos bereitstellen müssen, um dann von den „Vorteilen der Gesichtserkennung zu profitieren".

Iwashita erklärte: „Durch die Einführung der Gesichtserkennung hoffen wir, hohe Sicherheit, Effizienz und reibungslosen Betrieb an Sicherheits-Checkpoints zu erreichen." Die Veranstalter wollen damit insbesondere die Wartezeiten verkürzen. Tests im Vorjahr hätten gezeigt, dass Checkpoints mit Gesichtserkennung mehr als doppelt so schnell arbeiten wie konventionelle Systeme. Dadurch sollten die Spiele letztlich für die AthletInnen stressfreier werden, etwa indem ihnen unnötiges langes Schlangestehen bei großer Hitze erspart wird. Die Überprüfung soll nur 0,3 Sekunden dauern. ZuschauerInnen sind davon nicht betroffen.

Zum Einsatz kommt eine auf die Olympischen Spiele zugeschnittene Version der NEC-Gesichtserkennungstechnologie NeoFace. Diese wurde dem Unternehmen zufolge bereits in Rio 2016 getestet und vom U.S. National Institute of Standards and Technology 2017 als beste Video-Gesichtserkennungslösung bewertet. Biometriesysteme von NEC kommen dem Konzern zufolge mittlerweile in 70 Ländern unter anderem auf Flughäfen zum Einsatz. Im Sportbereich nutzt beispielsweise schon die Frauen-Profigolf-Tour LPGA NeoFace als Teil ihres Sicherheitskonzepts (Tokio 2020 setzt auf Gesichtserkennung, www.pressetext.com 07.08.2018; Gesichtserkennung in Tokio SZ 08.08.2018, 25).

Thailand

Biometrische Identifikation löst „alte Fälle"

Die Strafverfolgungsbehörde und die Polizei in Bangkok/Thailand haben eine Datenbank mit DNA und Fingerabdrücken von 48.708 Gefängnisinsassen erstellt und damit bei der Aufklärung von 46 bisher ungelösten Straffällen beigetragen. Polizei-Oberst Narat Sawettanan berichtete nach einer Diskussion mit Generalleutnant Panomporn Itthiprasert vom Büro für Forensische Wissenschaft über die neue Datenbank, die Fortschritt bei der Lösung „kalter Fälle" gebracht habe. Einige Insassen müssten sich für Verbrechen verantworten, für die sie derzeit nicht inhaftiert sind. Aufgeklärt worden seien so nationale Sicherheitsvorfälle, Diebstähle und sexuelle Straftaten (DNA und Fingerabdrücke: „Kalte Fälle" aufgeklärt, der-farang.com 26.10.2018).

Südkorea

Kampagne gegen „Spycam-Epidemie"

Am ersten September-Wochenende 2018 kündigten Behörden der südkoreanischen Hauptstadt Seoul an, dass 8.000 städtische Mitarbeitende auf Spycam-Jagd geschickt werden. Mit der dreimonatigen Razzia soll eine „Spycam-Epidemie" insbesondere auf öffentlichen Toiletten, in Umkleidekabinen

von Kaufhäusern und Hotelzimmern bekämpft werden. Dort werden winzige Kameras angebracht, oft nur für eine Viertelstunde, mit denen heimlich Filmchen aufgenommen werden, die dann später auf koreanischen Porno-Webseiten auftauchen. Die Porno-Webseiten, von denen es in Südkorea insgesamt ca. 4.000 geben soll, zahlen viel Geld für obszöne Filmschnippchen. Die Regierung von Präsident Moon Jae-in hatte schon im Juni 2018 eine Kampagne gegen Spycams ausgerufen.

Die Hemdknopf-großen Geräte selbst sind nicht verboten. Sie werden auch in Schreibstiften, Brillen und Ladegeräten eingebaut und sind kaum aufzuspüren. Bevor die Regierung die Gesetze verschärft hatte, hatte manch ein Krimineller 1.000 Filmchen hochgeladen und damit bis zu hundert Millionen Won (ca. 75.000 Euro) eingenommen. Wer erwischt wurde, zahlte bisher ein Bußgeld von etwa 40 Euro. Im Zuge der Kampagne sollen auch die Betreiber pornografischer Webseiten überprüft werden. Die Industrie Südkoreas entwickelt immer leistungsfähigere Technologien, doch die Gesellschaft ist darauf überhaupt nicht vorbereitet.

Das Phänomen der besonders perfiden Form des Voyeurismus, das in Südkorea Molka genannt wird, ist nicht neu. Schon 2011 wurden 2.000 Fälle strafrechtlich verfolgt, 2017 waren es 6.300 Fälle. 90% der Opfer sind Frauen. Neu dagegen ist die kollektive Empörung über Molka. Seit Mai 2018 gab es in Seoul vier große Demonstrationen, die letzte mit 70.000 TeilnehmerInnen, unter dem Motto „Unser Leben ist nicht euer Porno". Auch die #MeToo-Bewegung ist im März 2018 in Südkorea angekommen. Seither sind mehrere prominente Männer öffentlich entlarvt worden. Doch hatte die Polizei im Frühjahr 2018 auch eine junge Frau verhaftet, ein Fotomodell, weil sie einen männlichen Kollegen nackt gefilmt und den Film auf eine feministische Webseite gestellt hatte. Kurz darauf ging die Polizei gegen die feministische Webseite vor, während sie die üblichen Porno-Seiten gewähren ließ. Gegen Molka durch Männer wurde lange Zeit kaum etwas unternommen. Ein Gericht sprach im Sommer 2018 einen Politiker von allen Vorwürfen der Vergewaltigung und Belästigung frei, obwohl dieser zumindest letztere öffentlich halbwegs eingestanden hatte. Die großen Demonstrationen richteten sich deshalb nicht nur gegen Molka, sie prangerten die fehlende Gleichbehandlung der Geschlechter an: „Auch Frauen, nicht nur Männer, sind Bürger."

Molka und ähnliche pornografische Phänomene in Ländern wie Südkorea oder auch Japan sind kein Indiz dafür, dass diese Länder und diese Gesellschaften besonders sexualisiert sind, sondern eher ein Anzeichen für sexuelle Verklemmtheit. Untersuchungen von Kondom-Herstellern haben gezeigt, dass diese im Kern sehr konservativen Gesellschaften im weltweiten Vergleich fast am wenigsten Sex haben: Mehr als die Hälfte der verheirateten Paare in Japan sollen sogar gar keinen Sex miteinander haben. Zwei Drittel der jungen Männer sehen sich selbst als sogenannte „herbivor", also Personen, die gar keinen physischen Sex haben wollen. In Korea heißen sie „Blumen-Jungs". Viele von ihnen weichen offensichtlich auf Internet-Pornografie aus (Neidhart, „Unser Leben ist nicht euer Porno", SZ 05.09.2018, 10).

Südkorea

Verfassungsgericht: polizeiliche DNA-Datenbank ist verfassungswidrig

Das Verfassungsgericht Südkoreas entschied am 04.09.2018, dass das derzeit im Einsatz befindliche System zur Sammlung und Speicherung von personenbezogenen Geninformationen für polizeiliche Ermittlungen verfassungswidrig ist. Mit 6 gegen 3 Stimmen votierte das aus 9 Richtern bestehende Gericht, dass es inakzeptabel ist, dass die Strafverfolgungsbehörden einseitig DNA-Proben von Verdächtigen sammeln, ohne dass diesen die Möglichkeit eingeräumt wird, sich hiergegen zur Wehr zu setzen. Die Entscheidung geht auf die Klage von zivilgesellschaftliche Gruppen zurück, die kritisierten, dass bei der Speicherung von DNA-Daten diskriminierend vorgegangen werde, indem vorrangig Menschen aus sozialen Randgruppen, aus Gewerkschaften oder Ausgewiesene erfasst werden. Derzeit ist es der Polizei erlaubt, Genproben aus Blut, Speichel oder Haaren von Verurteilten oder inhaftierten Verdächtigen zu sammeln, nachdem eine entsprechende gerichtliche Anordnung erlassen wurde. Bei dem Verfahren wird den Betroffenen keine förmliche Möglichkeit zugestanden, hiergegen etwas vorzubringen. Die Daten werden dann unbefristet in der Polizeidatenbank gespeichert.

Der Fall wurde von einer Straßenverkäufervereinigung und einer Metallarbeitergewerkschaft vor Gericht gebracht. Beide Organisationen beanstandeten, dass von deren Mitglieder zwangsweise genetische Informationen erfasst wurden, nachdem sie wegen eines Sitzstreik-Protests und einer Besetzung privater Grundstücke verurteilt worden waren. Das Gericht stellte fest: „Das geltende Gesetz sieht nicht ausdrücklich ein Verfahren vor, wonach die Gerichte beim Erlass einer entsprechenden Anordnung den Betroffenen direkte Möglichkeiten einräumen, der Gendatensammlung zu widersprechen. Das Gesetz ist zwar insofern rechtmäßig, dass es dem öffentlichen Interesse an der Erleichterung strafrechtlicher Ermittlungen und der Kriminalitätsvorsorge dient, doch führt das Fehlen ausreichender rechtlicher Sicherungen dazu, dass die Betroffenen als reine Kriminelle behandelt werden." Das Gericht forderte die Nationalversammlung auf, bis zum Jahresende das Gesetz zu überarbeiten (Suh-yoon, Court rules DNA collection procedure unconstitutional, www.koreatimes.co 04.09.2018).

China

Google verknüpft Suchanfragen mit Telefonnummern

Erstmals wurden vom US-Onlinemagazins „The Intercept" Details veröffentlicht, wie die an die Zensuranforderungen der chinesischen Regierung angepasste Suchmaschine von Google mit dem Codename „Dragonfly" aussehen könnte. Demgemäß speichert ein Prototyp der Google-Android-App beispielsweise zu jeder Suchanfrage die Telefonnummer des Nutzenden. Verlangen die Behörden die Herausgabe der

Informationen, können sie schnell und einfach herausfinden, wer wann nach unliebsamen Dingen gegoogelt hat. Zuvor war schon berichtet worden, dass Google für die chinesische Version seiner Suchmaschine eine Liste mit verbotenen Begriffen zusammengestellt hat. Unter anderem finden sich darauf die chinesischen Begriffe für „Studentenprotest", „Nobelpreis" und „Menschenrechte". Google plant offenbar, seine chinesische Zweigstelle nicht alleine aufzubauen, sondern als Joint-Venture mit einem chinesischen Unternehmen. Der Kuschelkurs mit der chinesischen Regierung ist innerhalb des Google-Imperiums nicht unumstritten: Mindestens fünf Mitarbeitende haben laut „The Intercept" wegen der China-Politik des Unternehmens gekündigt (Kaluppke, Bericht: Google verknüpft in China Suchanfrage und Telefonnummer, www.heise.de 16.09.2018).

Technik-Nachrichten

Genetische Bestimmung der Haarfarbe kommt voran

ForscherInnen haben auf der Suche nach Genen, die die Haarfarbe beeinflussen, das Erbgut von insgesamt knapp 300.000 Menschen durchkämmt. Bislang waren 13 Gene bekannt. Eine im Fachblatt „Nature Genetics" veröffentlichte Studie fand insgesamt 124 Genregionen, die über eine blonde, braune, schwarze oder rote Mähne mitbestimmen.

Manfred Kayser vom Medizinischen Zentrum der Erasmus Universität Rotterdam, der die Studie mitgeleitet hat, meinte: „Das ist eine große Zahl." Bei vorherigen Analysen mussten sich die Forschenden mit Erbgutproben von wenigen tausend Menschen begnügen, deren Haarfarbe ihnen bekannt war. Dabei lassen sich nur Gene finden, die einen relativ großen Einfluss auf das Merkmal Haarfarbe haben. Doch 13 Gene konnten allein nicht komplett erklären, wie das Erbgut den Haaren den Ton angibt. Zwillingsstudien zufolge hängt die Haarfarbe bis zu 97% vom Erbgut, kaum von Umwelteinflüssen ab. Gemäß dem Forschungsbericht haben Frauen im Durchschnitt helleres Haar als Männer. Schwarze und rote Haare konnten die Forschenden mit relativ hoher Genauigkeit vorhersagen. Für braune und blonde Haare waren die Prognosen weniger akkurat.

Kaysers Team arbeitete mit Timothy Spector vom King's College London und damit mit der britischen Biobank Initiative und der US-Firma 23andMe zusammen, die sowohl die Gendaten als auch Informationen über das äußere Erscheinungsbild von 133.238 beziehungsweise 157.653 Menschen mit europäischer Herkunft beisteuerten. In 124 Genregionen, eine davon auf dem Geschlechtschromosom „X", fanden die Forschenden Abweichungen, die die Erblichkeit von roten Haaren zu 35% erklären, das von blonden Haaren zu 25% und von schwarzen zu 26%.

Dass so viele Gene zu diesem wichtigen äußerlichen Merkmal von Menschen beitragen, kam für Kayser nicht unerwartet: „Es hätten auch noch mehr sein können." Wie genau die einzelnen Genvarianten zum Entstehen der Haarfarbe beitragen, soll weiter untersucht werden. Mehr als 100 Genregionen waren zuvor nicht mit menschlicher Pigmentierung in Zusammenhang gebracht worden. So gibt es beispielsweise solche, die üblicherweise die Apoptose regulieren, also das Selbsttötungsprogramm der Zellen, die nun aber auch zur Haarfarbe beitragen sollen. Auch was Gene für die Pigmentierung tun, die sonst das Wandern von Zellen steuern, ist bisher unbekannt.

Dass zumindest einige der neu entdeckten Haarfarb-Gene wohl auch die Augen- und Hautfarbe beeinflussen dürften, wäre hingegen wenig überraschend, so Kayser: „Schon von den zuvor bekannten 13 Haarfarbgenen wissen wir, dass alle außer einem alle drei Pigmentierungsmerkmale des Menschen beeinflussen." Das liegt daran, dass die Farbstoffe Eumelanin und Pheomelanin in Haut, Haar und Auge von den gleichen spezialisierten Zellen, den Melanozyten produziert werden. Sie stecken in der Haut und in den Haarwurzeln und auch in der Iris des Auges.

Kayser hofft, dass das neue Wissen sich positiv auf das Verständnis von Krankheiten auswirkt, die mit Pigmentierung zusammenhängen, etwa Hautkrebs. Darüber hinaus sollte sich allerdings auch das Herauslesen des äußeren Erscheinungsbildes eines Täters aus der DNA von Blut- und Spermaspuren eines Tatorts verbessern lassen, die sogenannte „DNA-Phänotypisierung".

Über hundert Genregionen können die Forschenden in der DNS(DNA)-Spur eines Täters ohnehin nicht überprüfen. Dafür finde sich, so Kayser, an einem Tatort in der Regel viel zu wenig Erbgut, das noch dazu meist in schlechtem Zustand ist: „Es gibt zwar Methoden, die Hunderttausende von Erbgutvarianten überprüfen können, aber dafür reicht eben die DNS-Menge und der Erhaltungszustand nicht aus." Kayser arbeitet im EU-Projekt „Visage" an Lösungen für diese technologische Hürde. Bis es soweit ist, werden im „HIresPlex"-Test für die Bestimmung von Augen- und Haarfarbe, den Kaysers Labor entwickelt hat, nur die 24 aussagekräftigsten Genvarianten abgefragt, um Merkmale aus Täter-DNS zu bestimmen. Eine Erweiterung der Methode, mit der sich nun zusätzlich auch die Hautfarbe bestimmen lässt, stellte Kayser Mitte April 2018 im Fachblatt „Forensic Science International: Genetics" vor. Dabei werden insgesamt 41 Erbgutvarianten abgefragt.

In Deutschland sind solche Tests für Strafverfolgungszwecke (noch) nicht anwendbar. Die Zulassung in Bayern für Zwecke der Gefahrenabwehr ist hoch umstritten (DANA 2018, 18-25). Eine

Initiative der Bundesländer Bayern und Baden-Württemberg, die Strafprozessordnung zu ändern, ruht seit der Bundestagswahl. Kayser kritisiert: „Es ist eine vergebene Chance, die DNS-Phänotypisierung in Deutschland nicht zu nutzen." Andere Länder in Europa seien weniger zurückhaltend. In der Schweiz soll das Thema noch in diesem Jahr im Nationalrat diskutiert werden. Und in Staaten wie Schweden, Spanien oder Polen könne DNS ohnehin wie jede andere Tatort-Spur auch untersucht werden. Dort ist nur das Speichern von Erbgutdaten eingeschränkt, was bei der DNS-Phänotypisierung nicht nötig sei. In den Niederlanden, wo der gebürtige Berliner Kayser forscht, war die Gesetzgebung schneller als die Forschung. Das Parlament hatte schon Rahmenbedingungen beschlossen, bevor die forensischen Techniken existierten. Demnach können – nach parlamentarischer Prüfung – alle äußerlich erkennbaren Merkmale, die etwa auch ein Augenzeuge berichten könnte, aus Täter-DNS ermittelt werden (Karberg, Mehr als 120 Gene entscheiden über die Haarfarbe, www.tagesspiegel.de 17.04.2018; 124 Gene, SZ 17.04.2018, 14).

Rechtsprechung

EGMR

Großbritannien wegen GCHQ-Massenüberwachung verurteilt

Eine Kammer des Europäischen Gerichtshofs für Menschenrechte (EGMR) hat am 13.09.2018 Großbritannien wegen der massenhaften Ausspähung von JournalistInnen und AktivistInnen als Verstoß gegen die Grundrechte auf Meinungs- und Pressefreiheit sowie auf Schutz des Privatlebens (Art. 10 und 8 Europäische Menschenrechtskonvention – EMRK) verurteilt (Nr. 58170/13, 62322/14, 24960/15). Die Überwachung hatte der frühere US-Geheimdienstmitarbeiter, Computerexperte und Whistleblower Edward Snowden 2013 enthüllt. Betroffen waren unter anderem ein Netzwerk von investigativen JournalistInnen, die Bürgerrechtsorganisation Big Brother Watch und Nichtregierungsorganisationen. 16 von ihnen hatten in Straßburg Klage eingereicht. Prüfungsgegenstand des Gerichts war nicht nur die Überwachungspraxis, sondern auch das diese legitimierende Gesetz, der Regulation of Investigatory Powers Act (RIPA) aus dem Jahr 2000. Eine Strafe droht der britischen Regierung durch das Urteil nicht. Allerdings muss der Staat einen Teil der Verfahrenskosten erstatten, insgesamt 185.000 €. Schadenersatzforderungen gab es nicht. Das Urteil kann innerhalb von drei Monaten angefochten werden.

Gemäß dem Urteil verletzt die massenhafte Ausspähung die in der Europäischen Menschenrechtskonvention (EMRK) verbrieften Rechte auf freie Meinungsäußerung sowie auf Schutz des Privatlebens der VertreterInnen der Presse und der Bürgerrechtsorganisationen (Art. 10, 8 EMRK). Die Überwachung durch den britischen Geheimdienst GCHQ sei keiner „angemessenen und unabhängigen Kontrolle" unterworfen. Die Kriterien für die Auswahl der untersuchten Mails seien nicht klar definiert. Dies wiege umso schwerer, als dass die fraglichen Kommunikationen „sehr viele Dinge über die Gewohnheiten und die Kontakte" der überwachten Personen enthüllten. Einen Verstoß gegen Art. 6 EMRK sah das Gericht nicht, womit ein Recht auf gerichtliches Gehör garantiert werden soll.

„Besonders besorgt" zeigte sich der Gerichtshof über die Bedingungen, unter denen „vertrauliche Informationen von Journalisten gezielt zur Überprüfung ausgesucht werden können". Die Überwachungsbehörden könnten so Zugang zu den Quellen der Presse erlangen. Allein diese Möglichkeit könne „eine abschreckende Wirkung" auf Journalistinnen haben und somit die Pressefreiheit (Art. 10 EMRK) einschränken.

Hinzu komme, dass das britische Überwachungsgesetz einer großen Zahl von Behörden die Möglichkeit gebe, unter unzureichend definierten Bedingungen bei den Telekommunikationsunternehmen Zugang zu den Kommunikationen ihrer KundInnen zu beantragen. Dies gelte auch für die Kommunikation von JournalistInnen. Dies verstoße gegen eine Regelung der EU, wonach Kommunikationsunternehmen solche Informationen nur zum Zweck der Verbrechensbekämpfung weitergeben dürfen, und dies nur unter Kontrolle eines Gerichts oder einer anderen unabhängigen Stelle. Als Mitglied der Europäischen Union sei Großbritannien verpflichtet, deren Vorschriften einzuhalten.

Silkie Carlo, Direktorin von Big Brother Watch, zeigte sich mit dem Richterspruch zufrieden: „Unter dem Vorwand der Terrorbekämpfung hat das Vereinigte Königreich eines der autoritärsten Überwachungssysteme der westlichen Staaten eingeführt. Dieses Urteil ist ein wichtiger Schritt, um Millionen von rechtschaffenen Bürgern vor ungerechtfertigten Eingriffen in ihr Privatleben zu schützen."

2013 hatte Edward Snowden enthüllt, dass der britische Geheimdienst GCHQ in großem Umfang Informationen aus Kabeln abzweigte, über die die Kommunikationsdaten zwischen Großbritannien und den USA fließen. Die Erkenntnisse wurden zum Teil mit US-Geheimdiensten ausgetauscht. Dies ist gemäß dem Gericht rechtens. Die Regeln dafür seien ausreichend klar formuliert gewesen. Anzeichen für Missbrauch gebe es nicht. Seit der Enthüllung hat es umfangreiche Gesetzesänderungen gegeben. Das Innenministerium in London erklärte, es seien mehrstufige Verfahren eingeführt worden, um die Überwachung zu begrenzen. Zudem sei der Pos-

ten eines unabhängigen Beauftragten geschaffen worden, der die Einhaltung der Vorschriften kontrolliere. Gegen den Whistleblower Snowden liegt ein internationaler Haftbefehl vor. Er lebt derzeit in Russland im Asyl (European Court of Human Rights, Press Release ECHR 299 (2018) v. 13.09.2018, Some aspects of UK surveillance regimes violate Convention; Gericht verurteilt Großbritannien wegen Massen-Ausspähung von Journalisten, www.tagesspiegel.de 13.09.2018; Großbritannien wegen Massenüberwachung verurteilt, www.zeit.de 13.09.2018; Verletzte Rechte, SZ 14.09.2018, 37).

EuGH

Geringer Grundrechtseingriff rechtfertigt Nutzung von TK-Verkehrsdaten

Gemäß einem Urteil des Europäischen Gerichtshofs (EuGH) vom 02.10.2018 dürfen europäische Behörden zur Aufklärung wenig schwerer Straftaten auf gespeicherte Telekommunikations-(TK-)Verkehrsdaten zugreifen, wenn der damit verbundene Eingriff in die Privatsphäre weniger schwer wiegt (C-207/16). Damit erfolgte eine Präzisierung seines Urteils vom 21.12.2016 (C-203/15 u. C-698/15, DANA 2017, 60 f.). Im vorliegenden Fall ging es um den Raub einer Handtasche in Spanien und um die Frage, ob die Ermittlungsbehörden die Herausgabe jener Daten einfordern dürfen, die ab dem Raub für bis zu zwölf Tage vom Provider gesammelt wurden. Dies wurde vom EuGH bejaht.

Gemäß dem Urteil ist der Zugriff auf solche Daten beim Provider ein schwerer Eingriff in die Privatsphäre. Nur in Ausnahmefällen, etwa aus Gründen der nationalen Sicherheit, zur Wahrung der öffentlichen Sicherheit oder für die Landesverteidigung dürfen Mitgliedstaaten diese Rechte der Bürger einschränken. Im vorliegenden Fall gehe es aber nicht um einen solchen Tatbestand. Aus dem gewünschten Datenzugriff ließen sich keine genauen Schlüsse auf das Privatleben der Eigentümerin des Handys ziehen, da es nur um Daten geht, die gesammelt wurden, nachdem ihr das Gerät gestohlen worden war. Darin liege kein „schwerer Eingriff" in die Grundrechte. Der Datenzugriff erfolge zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung einer „Straftat" im Allgemeinen und sei dadurch gerechtfertigt.

Im Dezember 2016 hatte der EuGH die Regelungen zur TK-Vorratsdatenspeicherung in Großbritannien für grundrechtswidrig erklärt. Das Unionsrecht stehe grundsätzlich einer nationalen Regelung entgegen, „die eine allgemeine und unterschiedslose Speicherung von Daten vorsieht". Bestimmte Daten werden von Providern aber etwa für die Abrechnung eine gewisse Zeit gespeichert. In engen Grenzen ist dem EuGH zufolge dann auch ein behördlicher Zugriff auf diese Daten erlaubt (Holland, EuGH zur Vorratsdatenspeicherung: Behördenzugriff fallweise leichter, www.heise.de 02.10.2018).

EuGH

Urheberrechtsverstoß bei Neuveröffentlichung von Internet-Foto

Der Europäische Gerichtshof (EuGH) entschied am 07.08.2018, dass die Veröffentlichung eines Fotos auf einer Webseite ohne eine neue Zustimmung des Fotografen urheberrechtlich unzulässig ist, auch wenn das Foto im Internet frei zugänglich war (Az. C-161/17). Ein Fotograf hatte das Land Nordrhein-Westfalen wegen eines auf der Homepage einer Schule des Landes eingestellten Bilds verklagt. Im Streitfall hatte eine Schülerin einer Gesamtschule im nordrhein-westfälischen Waltrop ein Foto der spanischen Stadt Córdoba für ein Referat verwendet, das sie aus einem Reiseportal im Internet kopiert und das Portal auch als Quelle benannt hatte. Mitsamt dem Foto wurde das Referat auf der Homepage der Schule veröffentlicht.

Der Fotograf wurde von dem Reiseportal nicht benannt, sah sich aber durch die Kopie in seinen Urheberrechten verletzt. Er hatte den Betreibern des Portals erlaubt, auf ihrer Website das Foto zu veröffentlichen. Der deutsche Bundesgerichtshof (BGH) in Karlsruhe hatte den Fall dem EuGH vorgelegt. Der BGH wollte vom EuGH in Luxemburg wissen, wie die Urheberrechtsrichtlinie in einem solchen Fall auszulegen ist. Konkret wollte der BGH wissen, ob der Begriff der „öffentlichen Wiedergabe" auch die Einstellung eines Fotos auf einer Website erfasst, wenn dieses zuvor ohne Beschränkung und mit Zustimmung des Urheberrechtsinhabers auf einer anderen Seite veröffentlicht wurde. Der EuGH bejahte diese Frage. Denn dadurch werde das Bild einem „neuen Publikum" zugänglich gemacht (Enge Grenzen bei Verwendung fremder Fotos auch auf Schulhomepage, www.epochtimes.de 07.08.2018).

BGH

Unterlassungsanspruch begründet keine Pflicht zur umfassenden Internetbereinigung

Der Bundesgerichtshof (BGH) in Karlsruhe entschied in einem Beschluss vom 12.07.2018, dass eine Rundfunkanstalt, die gerichtlich zur Entfernung eines fehlerhaften Beitrags verpflichtet worden ist, diesen lediglich aus der eigenen Mediathek entfernen und sicherstellen muss, dass gängige Suchmaschinen den Beitrag in ihren Suchergebnissen nicht auffindbar machen (I ZB 86/17). Konkret ging es um einen Fernsehbeitrag der NDR-Sendung „Markt" vom 13.03.2017 mit dem Titel „Wirbel um belasteten Bauschutt in Hannover". Eine darin genannte Person erwirkte wegen verschiedener Äußerungen in dem Beitrag eine gerichtliche Unterlassungsverfügung. Danach durfte der Fernsehsender diesen nicht weiter verbreiten oder verbreiten lassen.

Der NDR entfernte den Beitrag aus seiner Mediathek und beantragte dessen Löschung bei den gängigen Internetsuchmaschinen, insbesondere Google. Doch auf Youtube hatte eine dritte Person den Beitrag ebenfalls veröffentlicht, wo er mindestens 153mal aufgerufen wurde. Der Antragsteller meinte, dass der NDR gegen die Unterlassungsverfügung verstoßen habe. Der Beitrag sei weiter verbreitet worden. Das Landgericht Hannover verhängte deshalb gegen den Sender ein Ordnungsgeld in Höhe von 5.000 Euro. Die sofortige

Beschwerde des NDR führte aber dazu, dass das Oberlandesgericht (OLG) Celle den Vollstreckungsantrag zurückwies.

Der BGH wies die Rechtsbeschwerde gegen die OLG-Entscheidung zurück. Mit der Unterlassungsverfügung sei der NDR verpflichtet worden, den Fernsehbeitrag aus seiner Mediathek zu entfernen. Auch müsse der Sender auf die gängigen Suchmaschinen einwirken, dass der Beitrag nicht mehr in den Suchergebnissen erscheint. Die Unterlassungspflicht werde aber grundsätzlich nicht verletzt, wenn ein Dritter den Beitrag selbstständig in einem Internetvideoportal veröffentlicht. Der NDR müsse auch nicht anlassunabhängig Videoplattformen und soziale Medien dahingehend durchforsten, ob andere Personen den Beitrag rechtswidrig veröffentlicht haben. Nur bei Kenntnis müsse er auf eine Entfernung des Beitrags – hier bei Youtube – hinwirken. Dem sei der NDR nachgekommen (NDR muss Youtube nicht nach zu löschenden Beiträgen durchsuchen, chrismon.evangelisch.de 28.09.2018).

BGH

Zufriedenheitsbefragung ist Werbung

Eine Kundenzufriedenheitsbefragung per E-Mail ist gemäß einem Urteil des Bundesgerichtshofs (BGH) vom 10.07.2018 als Werbung auch dann unzulässig, wenn sie mit der Rechnung für ein gekauftes Produkt versendet wird (VI ZR 225/17-LG Braunschweig). Der BGH klärte damit, inwieweit die Verknüpfung des Versands einer Rechnung per E-Mail mit der Bitte um eine Zufriedenheitsbewertung in derselben Mail zulässig ist. Geklagt hatte ein Kunde, der über die Internet-Plattform „Amazon Marketplace" Ware bestellt hatte. Die Abwicklung des Geschäfts erfolgte über Amazon. Im Nachgang hatte der Verkäufer die Rechnung mit einer E-Mail versendet, in der er sich außerdem für den Kauf bedankte und um eine gute Bewertung bat, falls der Käufer mit dem Service zufrieden gewesen sei. Der Käufer sah in dieser E-Mail eine unaufgeforderte unerlaubte Zusendung von Werbung, die in sein allgemeines Persönlichkeitsrecht eingreife.

Das Amtsgericht Braunschweig hatte die Klage zunächst abgewiesen, ebenso das Berufungsgericht, das aber eine Revision und damit ein Weiterverfolgen des Klagebegehrens zuließ. Der BGH entschied zugunsten des Klägers: Das Versenden von Werbung per elektronischer Post ist grundsätzlich ein Eingriff in die Privatsphäre des Empfängers und damit in sein allgemeines Persönlichkeitsrecht, wenn dies ohne vorherige Einwilligung des Empfängers erfolgt. Eine Kundenzufriedenheitsbefragung fällt auch dann unter den Begriff der (Direkt-)Werbung, wenn sie zusammen mit der Rechnung für ein gekauftes Produkt versendet wird. Denn, so der BGH, es ist für den Verkäufer zumutbar, nach Abschluss der geschäftlichen Transaktion gemäß § 7 Abs. 3 Gesetz gegen den unlauteren Wettbewerb (UWG), dem Empfänger die Möglichkeit einzuräumen, einer Verwendung seiner E-Mail-Adresse für Werbung zu widersprechen, bevor er mit einer Werbemail in dessen Privatsphäre eindringt. Anderenfalls ist der Eingriff grundsätzlich rechtswidrig. Der Beklagte wurde zur Unterlassung verurteilt, bei Zuwiderhandlung ist ein vom Gericht festzusetzendes Ordnungsgeld von bis zu 250.000 Euro, ersatzweise Ordnungshaft von bis zu sechs Monaten am Geschäftsführer zu vollziehen (Roos, BGH-Urteil: Kundenzufriedenheitsumfrage unzulässig, www.heise.de. 16.09.2018).

BGH

Bild muss Schmerzensgeld an Kachelmann zahlen

Der Bundesgerichtshof (BGH) entschied mit Beschluss vom 23.07.2018 über eine Beschwerde des Medienkonzerns Axel Springer wegen der Verletzung von Persönlichkeitsrechten von Wettermoderator Jörg Kachelmann (VI ZR 352/16). Gegenstand der beanstandeten Berichterstattung von „Bild" waren Vergewaltigungsvorwürfe, von denen Kachelmann 2011 freigesprochen wurde. Dieser nahm den Medienkonzern in Höhe von insgesamt 530.000 Euro in Anspruch. Die Axel Springer SE hatte beanstandet, dass eine Revision gegen ein Urteil des Oberlandesgerichts Köln vom 12.07.2016 (15 U 175/15) nicht zugelassen war. Das Urteil wird nun rechtskräftig und eine Schmerzensgeld-Entschädigung in Höhe von rund 235.000 Euro fällig, inklusive Schadensersatz und Zinsen seit August 2010. Ein Springer-Sprecher erklärte zunächst, man habe die Entscheidung „mit Bedauern zur Kenntnis genommen". Da sie „der Bedeutung der grundrechtlich geschützten Berichterstattung nicht angemessen" sei, prüfte man die Möglichkeit einer Verfassungsbeschwerde (Bongen, „Bild" muss Kachelmann erneut Schmerzensgeld zahlen, www.ndr.de 26.09.2018; Schmerzensgeld für Kachelmann SZ 16.04.2018, 25).

BAG

Kein Verwertungsverbot von Videobildern bei längerer Speicherung

Das Bundesarbeitsgericht (BAG) entschied mit Urteil vom 24.08.2018, dass die Speicherung von Bildsequenzen aus einer rechtmäßigen offenen Videoüberwachung, die vorsätzliche Handlungen einer Arbeitnehmerin zulasten des Eigentums des Arbeitgebers zeigen, nicht durch bloßen Zeitablauf unverhältnismäßig wird, solange die Ahndung der Pflichtverletzung durch den Arbeitgeber arbeitsrechtlich möglich ist (2 AZR 133/18). Die Klägerin war in einem vormals von dem Beklagten betriebenen Tabak- und Zeitschriftenhandel mit angeschlossener Lottoannahmestelle tätig. Dort hatte der Beklagte eine offene Videoüberwachung installiert. Mit den Aufzeichnungen wollte er sein Eigentum vor Straftaten sowohl von KundInnen als auch von eigenen Beschäftigten schützen. Im 3. Quartal 2016, also von Juli an, stellte die Beklagte einen Fehlbestand bei Tabakwaren festgestellt. Bei einer im August 2016 vorgenommenen Auswertung der Videoaufzeichnungen durch zwei Mitarbeiterinnen, die insgesamt 10 Stunden gedauert haben soll, habe sich gezeigt, dass die Klägerin an zwei Tagen im Februar 2016 vereinnahmte Gelder nicht in die Registrierkasse gelegt habe. Dies ist auf

den Videos aber nicht zu sehen; die Unterschlagung wurde der Beschäftigten vorgeworfen, weil sie auf verdächtige Weise mit der Geldkassette in der Hand den Verkaufsraum verlassen und kurz danach wieder betreten hatte. Der beanstandete Fehlbetrag betrug 80,50 Euro. Der Beklagte kündigte daraufhin das Arbeitsverhältnis außerordentlich fristlos. Die Frau arbeitete auf 450-Euro-Basis und will mit ihrer Klage die Rücknahme ihres Rauswurfs erreichen. Der Laden, in dem sie arbeitete, ist allerdings mittlerweile geschlossen.

Ob die Frau das Geld tatsächlich unterschlagen hat, ist strittig. Die Vorinstanzen haben der dagegen gerichteten Kündigungsschutzklage stattgegeben. Das Arbeitsgericht Iserlohn fand durch die Videoaufnahmen den Nachweis nicht erbracht. Das LAG wollte sich mit dieser Frage gar nicht befassen, weil zwischen Aufnahme und Auswertung so viel Zeit vergangen war, dass die Bilder „keinen zulässigen Beweis für die Richtigkeit der Behauptungen" ergeben könnten. Es hatte am 20.12.2017 geurteilt, die Erkenntnisse aus den Videoaufzeichnungen unterlägen einem Verwertungsverbot (2 Sa 192/17). Der Arbeitgeber hätte die Bildsequenzen „unverzüglich", jedenfalls deutlich vor dem 01.08.2016 löschen müssen. Auf dessen Revision hob das BAG das LAG-Berufungsurteil hinsichtlich des Kündigungsschutzantrags auf und verwies die Sache zur neuen Verhandlung und Entscheidung an das LAG. Sollte es sich, was der BAG-Senat nach den bisherigen Feststellungen nicht beurteilen konnte, um eine rechtmäßige offene Videoüberwachung gehandelt haben, wäre die Verarbeitung und Nutzung der einschlägigen Bildsequenzen nach BAG-Ansicht gemäß § 32 Abs. 1 Satz 1 BDSG a. F. zulässig gewesen und hätte dementsprechend nicht das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht der Klägerin verletzt. Der beklagte Arbeitgeber hätte das Bildmaterial nicht sofort auswerten müssen: „Er durfte hiermit solange warten, bis er dafür einen berechtigten Anlass sah." Sollte die Videoüberwachung rechtmäßig erfolgt sein, stünden auch die Vorschriften der seit dem 25.05.2018 geltenden Datenschutz-Grundverordnung einer gerichtlichen Verwertung der erhobenen personenbezogenen Daten der Klägerin im weiteren Verfahren nicht entgegen.

Der Fall hat noch eine weitere Spezialität: Der Arbeitgeber kündigte seiner Mitarbeiterin nicht nur fristlos, sondern forderte die Erstattung der für ihre Überführung als Täterin entstandenen Kosten, insgesamt 430 Euro plus Zinsen. Das LAG hatte diese Forderung abgelehnt (BAG PM Nr. 40/18, Offene Videoüberwachung – Verwertungsverbot v. 23.08.2018; Esslinger, Der Chef schaut zu, SZ 24.08.2018, 5).

OVG Münster

Ausweiskontrolle wegen Hautfarbe rechtswidrig

Das Oberverwaltungsgericht (OVG) Münster hat am 07.08.2018 geurteilt, dass die Personenkontrolle eines Mannes durch zwei Beamte unter anderem wegen seiner dunklen Hautfarbe rechtswidrig war (5 A 294/16). Der heute 43-Jährige war im November 2013 am Bochumer Hauptbahnhof kontrolliert worden, seiner Ansicht nach wegen seiner dunklen Hautfarbe. Der Wittener verklagte die Bundespolizei und bekam Recht.

Das OVG entschied, dass diese Ausweiskontrolle ein Verstoß gegen das im Grundgesetz verankerte Diskriminierungsverbot war. In der mündlichen Urteilsbegründung wurde betont, dass Polizeibeamte nur dann auch die Hautfarbe als Anknüpfungspunkt für eine Kontrolle auswählen dürfen, wenn ausreichende Anhaltspunkte für Straftaten vorliegen. Dafür könnten beispielsweise fundierte Kriminalitätsstatistiken benutzt werden. Der Rechtsvertreter der Polizei konnte allerdings im Verfahren keine überzeugenden Kriminalitätsstatistiken für den Hauptbahnhof Bochum vorlegen. Aus den vorgelegten Statistiken ergab sich, dass der Großteil der registrierten Straftaten für den Bochumer Bahnhof auf das Konto von Deutschen ging. Richterin Riccarda Brandts erläuterte: „Die bloße Behauptung, dass zum Großteil Nordafrikaner für Eigentumsdelikte verantwortlich sind, reicht nicht. Die Behörde hat eine erhöhte Darlegungslast." Auch habe es sich nicht um eine illegale Einreise handeln können: „Der Kläger hat den Bahnhof ja von außen betreten." Die Polizei hatte argumentiert, der Mann habe sich auffällig verhalten und das sei damals auch ein Grund für die Kontrolle gewesen. Das Gericht, das mit seiner Entscheidung ein Urteil des Verwaltungsgerichts Köln aus der ersten Instanz von 2016 (20 K 7847/13) kippte, ließ keine Revision zum Bundesverwaltungsgericht zu. Das sogenannte „Racial Profiling" ist rechtswidrig (Personenkontrolle wegen Hautfarbe in Bochum war rechtswidrig, www1.wdr.de 07.08.2018; Ausweiskontrolle wegen Hautfarbe rechtswidrig SZ 08.08.2018, 5).

OLG Köln

Recht am Bild nach KUG gilt weiterhin

Das Oberlandesgericht (OLG) Köln hat mit einer Entscheidung vom 18.06.2018 festgestellt, dass mit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) das Kunsturhebergesetz (KUG) für die Medienberichterstattung gültig bleibt (15 W 27/18). Es war schon bisher unzulässig, Aufnahmen von Personen ohne deren Einwilligung zu veröffentlichen. § 23 KUG regelt einige Ausnahmen: Bildnisse der Zeitgeschichte, Fotos von Großereignissen oder Aufnahmen, in denen die Personen nur als Beiwerk des eigentlichen Inhalts zu sehen sind. Ob eine solche Ausnahme vorliegt, müssen im Zweifel die Gerichte klären. Mit der Wirksamkeit der DSGVO stellte sich die Frage, ob nun grundsätzlich die Zustimmung jedes Abgebildeten notwendig ist.

Das OLG wies darauf hin, dass der europäische Gesetzgeber mit Artikel 85 DSGVO den nationalen Gesetzgebern einen Gestaltungsspielraum gelassen hat, da ein Spannungsfeld zwischen Datenschutz einerseits und journalistischer Berichterstattung andererseits besteht. Um diesen Widerspruch auszugleichen, darf ein Land eigene Regelungen finden. Das Gericht stellte klar, dass mit dem Art. 85 verhindert werden soll, dass der Datenschutz die Meinungs- und Kommunikationsfreiheit einschränkt.

Die nationalen Regelungen in ein neues Gesetz zu fassen, schreibe die DS-

GVO nicht vor. Mit dem Kunsturhebergesetz verfüge man in Deutschland über ein geeignetes Mittel zur Ausgestaltung des Art. 85. Die Regelung lasse zahlreiche Abwägungsmöglichkeiten zu. Auch europarechtliche Aspekte könnten hier zur Geltung kommen. Dies bedeutet, dass für den begrenzten Bereich der Veröffentlichung von Fotos zur journalistischen Berichterstattung auch nach Wirksamwerden der DSGVO das KUG die Handlungsrichtlinien vorgibt. Nicht erfasst von dem Urteil ist allerdings der vorhergehende Schritt: das Anfertigen von Fotos, das ebenfalls als Verarbeitung von Daten im Sinne der DSGVO anzusehen ist. Auch über das Onlinestellen zu nicht-journalistischen Zwecken durch Künstler, Unternehmen, Blogger oder Privatpersonen hat das Gericht keine Aussage getroffen (Evers, DSGVO-Urteil: Bei Veröffentlichung journalistischer Fotos gilt Kunsturhebergesetz, www.e-recht24.de 02.07.2018).

VG Bayreuth

Gehashter E-Mail-Adressenabgleich über Facebook Marketing Tool ohne Einwilligung unzulässig

Mit Beschluss vom 08.05.2018 entschied das Verwaltungsgericht (VG) Bayreuth im Rahmen eines einstweiligen Rechtsschutzverfahrens, dass die Bildung einer „Custom Audience“ bei Facebook durch Hochladen einer gehashten Email-Liste datenschutzrechtlich unzulässig ist (Az. B 1 S 18.105). Dabei handelt es sich um eine Überschneidungsanalyse zwischen Nutzerdaten der Plattform und gehashten Daten von Online-Shops. Die kurz vor dem Inkrafttreten der DSGVO gefällte Entscheidung erfolgte noch auf der Grundlage des alten Bundesdatenschutzgesetzes (BDSG), ist aber inhaltlich voll auf die neue Rechtslage übertragbar. Das Bayerische Landesamt für die Datenschutzaufsicht (BayLDA) durfte zur Gewährleistung des Datenschutzrechts Maßnahmen zur Beseitigung festgestellter Verstöße bei der personenbezogenen Datenverarbeitung anordnen.

Personenbezogene Daten sind danach auch gegeben, wenn ein „Hashen“ erfolgt, da der Personenbezug hierdurch nicht völlig aufgehoben wird. Es ist weiterhin mit nicht nur unverhältnismäßigem Aufwand möglich, die Daten einer bestimmten oder bestimmbaren Person zuzuordnen, zumal andernfalls auch ein sich an die Übermittlung anschließender Datenabgleich seitens Facebook nicht möglich wäre. Das VG trat dem Standpunkt des BayLDA bei, wonach es sich bei der Übermittlung der gehashten E-Mail-Adressen der Kunden der klagenden Onlineshop-Betreiberin nicht um eine Datenweitergabe im Rahmen einer Auftragsdatenverarbeitung handelt, sondern um eine Übermittlung an Dritte. Zwar betraute die Onlineshop-Betreiberin Facebook damit, Daten zu verarbeiten. Auf die Rechtsnatur dieser Betrauung kommt es dabei nicht an, ein Auftrag i. S. v. § 662 BGB ist nicht erforderlich. Facebook habe einen eigenen Wertungs- und Entscheidungsspielraum. Deshalb ging das VG bei vorliegenden Sachverhaltsgestaltung nicht von einer Auftragsdatenverarbeitung aus, sondern vielmehr von einer sog. „Funktionsübertragung“. Die Vereinbarung zwischen der Onlineshop-Betreiberin und Facebook bezog sich auf die Durchführung der Überschneidungsanalyse und die Erstellung einer Vergleichsaudience. Dabei handelt Facebook nicht als „verlängerter Arm“ der Onlineshop-Betreiberin, da es allein im Ermessen Facebooks liegt, dem insoweit ein entsprechender Spielraum eingeräumt wird, wer konkret beworben wird.

Das VG räumte ein, dass Gestaltungsmöglichkeit bestehen, wonach eine Stelle eine Doppelfunktion einnimmt und nebeneinander zugleich Auftragsdatenverarbeiterin und verantwortliche Stelle ist. Dies war hier aber nicht der Fall, da das Marketing Tool „Facebook Custom Audience über die Kundenliste“ einen einheitlichen Vorgang bildet und das Instrument nicht in verschiedene Teile zerlegt werden kann. Daran ändert sich nichts dadurch, dass sich der einheitliche Vorgang aus mehreren datenschutzrechtlich relevanten Vorgängen zusammensetzt. Die Übermittlung der (gehashten) E-Mail-Adressen ist integraler Bestandteil der Werbemaßnahme.

Für die Bewerbung einzelner Personen mit dem Werkzeug kommt es maßgeblich darauf an, dass Facebook diesen bestimmte Eigenschaften durch detaillierte Auswertung des Nutzungsverhaltens zuschreibt. Hierin liegt der Spielraum Facebooks, der über eine rein datenverarbeitende Hilfsfunktion, durch die eine Auftragsdatenverarbeitung gekennzeichnet ist, deutlich hinausgeht.

Im Verfahren des einstweiligen Rechtsschutzes nicht abschließend geklärt wurde die streitige Frage, ob und gegebenenfalls in welchem Umfang Facebook zu einer weiteren Nutzung der Daten berechtigt ist bzw. diese stattfindet (etwa durch eine „Anreicherung des Profils“). Das Gericht stellte aber klar, dass bei einer Überlassung der Nutzungsrechte an den Daten unzweifelhaft eine Funktionsübertragung stattfindet. Nach Durchführung des Abgleichs werden die übermittelten Informationen von Facebook nicht vollständig gelöscht, sondern registriert, dass der Betroffene Teil der Custom Audience der Onlineshop-Betreiberin ist. Die Onlineshop-Betreiberin stellte sich auf den Standpunkt, dass die Schritte, die nach dem Datenabgleich stattfinden, sich allein in der Zuständigkeit Facebooks vollziehen. Genau dies ist für das VG eine Bestätigung, dass hier eine Funktionsübertragung erfolgt.

Für eine Übermittlung der gehashten E-Mail-Adressen sah das VG keine Rechtsgrundlage. Es läge weder eine wirksame Einwilligung vor, noch könne sich die Onlineshop-Betreiberin auf das sog. „Listenprivileg“ stützen (§ 28 Abs. 3 S. 2 BDSG-alt), da es sich bei E-Mail-Adressen nicht um gesetzlich abschließend aufgezählte sog. Listendaten handelte. Das VG ließ das Vorbringen der Onlineshop-Betreiberin nicht gelten, dass in der Übertragung der gehashten E-Mail-Adressen nur die Information enthalten sei, dass jemand (möglicherweise) Kunde der Onlineshop-Betreiberin ist. Ebenso lehnte das VG die Argumentation ab, dass es sich bei der Übermittlung nur um ein „Hinzuspeichern“ handele oder um Werbung für fremde Angebote, was eine Übermittlung an Dritte ausschließt.

Auch im Rahmen einer Interessenabwägung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG-alt, die dem Art. 6 Abs. 1 lit. f DSGVO entspricht, sah das VG Bayreuth keine Rechtfertigung für die Datenübermittlung an Facebook. Dabei griff

das Gericht auf die Wertungen des § 28 Abs. 3 BDSG-alt zurück, wonach die Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Werbung grds. nur zulässig war, wenn der Betroffene eingewilligt hat. Hinsichtlich des Custom Audience von Facebook sah das Gericht ein Überwiegen der Betroffenenrechte. Es erfolge keine Nutzung für eigene Werbezwecke, sondern eine Übermittlung an Dritte. Die Stelle, die die Daten erstmalig erhoben hat, also die Onlineshop-Betreiberin, müsse wegen des Transparenzgebots eindeutig den konkreten Werbezweck erkennen lassen und der Weiterverarbeiter, woher er die Listen hat, etwa durch Angabe des Namens und der Anschrift des Adresshändlers. Nur so könne der Betroffene sein Widerspruchsrecht wahrnehmen. Der Umstand, dass es sich um Angebote der Onlineshop-Betreiberin handelt, die dem Betroffenen bei Facebook angezeigt werden, reicht insoweit nicht aus, zumal die Stelle, die die Daten zum Zwecke der Werbung verwendet und die, zu deren Gunsten die Werbung erfolgt, auseinanderfallen können (etwa bei der Beipack- und Empfehlungswerbung).

Auch die konkrete Ausgestaltung der Widerspruchsmöglichkeit wurde vom VG kritisiert. Die Onlineshop-Betreiberin führte aus, dass sie (erst) seit dem 22.08.2017 einen konkreten Hinweis auf die Übermittlung der E-Mail-Adressen an Facebook gibt. Früher erfasste Daten befänden sich eventuell nach wie vor auf der hochgeladenen Kundenliste, ohne dass sichergestellt ist, dass sie von den aktuellen Datenschutzhinweisen Kenntnis genommen haben.

Für die Zulässigkeit einer Datenübermittlung genüge nicht die Geeignetheit oder Zweckmäßigkeit zur Wahrung berechtigter Interessen, sondern deren Erforderlichkeit. Eine Berufung auf die Abwägungsklausel käme so lange nicht in Betracht, wie diese ihr Informationsziel anders erreichen kann. Der Onlineshop-Betreiberin sei es ohne einen unverhältnismäßig großen Aufwand möglich, im Einzelfall eine Einwilligung zur Übermittlung der Daten an Facebook einzuholen.

Wegen der Rechtswidrigkeit der Datenübermittlung an Facebook war das BayLDA berechtigt, von der Onlineshop-Betreiberin die Beseitigung des festgestellten Verstoßes zu verlangen, indem sie ohne erkennbare Ermessensfehler eine Löschungsanordnung verfügte (www.gesetze-bayern.de, Zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten; Benedikt, Bayerisches Verwaltungsgericht entscheidet über Einsatz von Facebook-Marketing-Tool, BvD-News 2/2018, 46 ff.).

LG Würzburg

DSGVO-Abmahnung gegen Rechtsanwalt

Das Landgericht hat mit Beschluss vom 13.09.2018 im Rahmen eines einstweiligen Verfügungsverfahrens wegen Dringlichkeit ohne mündliche Verhandlung folgenden Beschluss zur einer Abmahnung eines Anwaltes gegen eine Anwältin erlassen (11 O 1741/18 UWG):

„I. Der Antragsgegnerin wird untersagt, für ihre berufliche Tätigkeit als Rechtsanwältin die unverschlüsselte Homepage XXX ohne Datenschutzerklärung nach der Datenschutz-Grundverordnung der EU (DSGVO 2016/679) vom 27.04.2016 in deren Geltungsbereich zu betreiben.

II. Der Antragsgegnerin wird für jeden Fall der Zuwiderhandlung die Verhängung eines Ordnungsgeldes von bis zu 250.000,00 €, ersatzweise Ordnungshaft bis zu 2 Jahren, sowie die Verhängung einer Ordnungshaft von bis zu 6 Monaten angedroht.

... V. Der Streitwert wird auf 2.000,00 € festgesetzt.

Gründe: Die Zuständigkeit des Gerichts ergibt sich hier aus § 14 Abs. 2 UWG (Begehungsort, fliegender Gerichtsstands bezüglich des Internets) und nicht aus § 32 ZPO, wie von Antragstellerseite angegeben.

Dem Antragsteller steht ein Verfügungsanspruch auf Unterlassung zu, da der Antragsteller glaubhaft gemacht hat, dass die Antragstellerin bezüglich ihrer Homepage gegen die Datenschutzgrundverordnung (DSGVO), die spätestens seit 25.05.2018 umzusetzen ist, verstößt. Die im Impressum der Antragsgegnerin enthaltene 7-zeilige Datenschutzerklärung genügt der neuen DSGVO nicht. Es fehlen Angaben zum/zur Verantwortlichen, zur Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck deren Verwendung, eine Erklärung zur Weitergabe von Daten, über Cookies, Analysetools, aber vor allem die Belehrung über die Betroffenenrechte, insbesondere Widerspruchsrecht, Datensicherheit und ein Hinweis zur Möglichkeit, sich bei einer Aufsichtsbehörde zu beschweren. Mit dem OLG Hamburg (3 U 26/12) und dem OLG Köln (8 U 121/15) geht das erkennende Gericht davon aus, dass es sich bei den Vorschriften, gegen die hier verstoßen wurde, um Verstöße gegen das Wettbewerbsrecht gemäß § 4 Nr. 11 UWG bzw. jetzt § 3a UWG handelt und somit vom Antragsteller abgemahnt werden konnte. Dass die Antragsgegnerin Daten erhebt, wird schon aus der gleichzeitigen Verwendung eines Kontaktformulars auf der Homepage indiziert. Da die Antragsgegnerin jedenfalls über ein Kontaktformular Daten erheben kann, ist zwingend auch eine Verschlüsselung der Homepage erforderlich, die hier fehlt.

Gem. § 8 Abs. 3 UWG ist der Antragsteller aktiv legitimiert, die beanstandeten Gesetzesverstöße geltend zu machen. Es besteht das erforderliche Wettbewerbsverhältnis aufgrund der Möglichkeit, als Rechtsanwalt bundesweit tätig zu werden.

Die erforderliche Wiederholungsgefahr wird durch das rechtsverletzende Verhalten indiziert. Somit ist der Verfügungsanspruch gegeben.

Ein Verfügungsgrund ist bei wettbewerbsrechtlichen Unterlassungsansprüchen gem. § 12 Abs. 2 UWG indiziert. Nach Aufforderung des Gerichts hat der Antragsteller zudem glaubhaft gemacht, dass er innerhalb der von der Rechtsprechung angenommenen Monatsfrist erst von den Verstößen Kenntnis erlangt hat und dass somit keine Selbstwiderlegung der Dringlichkeit durch zu langes Zuwarten vorliegt.

Dem Antrag konnte nicht dahingehend entsprochen werden, der Antragsgegnerin eine vom Gericht festzusetzende Vertragsstrafe anzudrohen. Der Antragsgegnerin sind vielmehr für den Fall der Zuwiderhandlung gegen das erlassene Verbot die in § 890 Abs. 1 ZPO vorgesehenen Ordnungsmittel anzudrohen.

Das Gericht hat die einstweilige Verfügung wegen Dringlichkeit ohne mündliche Verhandlung erlassen, § 937 Abs. 2 ZPO. Eine Schutzschrift wurde im Übrigen nicht hinterlegt."

LG Bochum

Keine Wettbewerbsklage bei Datenschutzverstößen

Anders als – wie oben dokumentiert – das LG Würzburg entschied das Landgericht (LG) Bochum mit Teil-Versäumnis- und Schlussurteil vom 07.08.2018, dass Datenschutzverstöße von Wettbewerbern nicht abmahnfähig sind (I-12 O 85/18):

„Keinen Erfolg hatte der Antrag hingegen, soweit ein Verstoß gegen Artikel 13 der Datenschutzgrundverordnung geltend gemacht wird. Denn dem Verfügungskläger steht ein solcher nicht zu, weil die Datenschutzgrundverordnung in den Artikeln 77 bis 84 eine die Ansprüche von Mitbewerbern ausschließende, abschließende Regelung enthält. Die Kammer verkennt dabei nicht, dass diese Frage in der Literatur umstritten ist und die Meinungsbildung noch im Fluss ist. Die Kammer in ihrer derzeitigen Besetzung schließt sich der besonders von Köhler (ZD 2018, 337 sowie in Köhler/Bornkamm/Feddersen, UWG, 36. Aufl. 2018, § 3 a Rn. 1.40 a und 1.74 b, im Ergebnis auch Barth WRP 2018, 790; anderer Ansicht Wolff, ZD 2018, 248) vertretenen Auffassung an. Dafür spricht insbesondere, dass die Datenschutzgrundverordnung eine detaillierte Regelung des anspruchsberechtigten Personenkreises enthält. Danach steht nicht jedem Verband ein Recht zur Wahrnehmung der Rechte einer betroffenen Person zu, sondern nur bestimmten Einrichtungen, Organisationen und Vereinigungen ohne Gewinnerzielungsabsicht unter weiteren Voraussetzungen. Hieraus ist zu schließen, dass der Unionsgesetzgeber eine Erstreckung auf Mitbewerber des Verletzers nicht zulassen wollte (Köhler, ZD 2018, 337, 338). Wegen der weiteren Einzelheiten der Argumentation kann auf die zitierten Literaturstellen Bezug genommen werden."

Die Frage einer „Sperrwirkung" der DSGVO für wettbewerbsrechtliche Sanktionen ist nicht neu. Die EG-Datenschutzrichtlinie 1995 (DSRl) enthielt in den Art. 22 bis 24 DSGVO Regelungen zu Sanktionen, und in dem Düsseldorfer „Fashion ID"-Fall wandten die Beklagten seinerzeit ein, dass es eine „Sperrwirkung" der Art. 22 bis 24 DSRl gegenüber § 3a UWG gebe. Das OLG Düsseldorf hielt dies für so gewichtig, dass er dem EuGH in seinem Vorlagebeschluss vom 19.01.2017 (I-20 U 40/16) eine entsprechende Frage stellte:

„Steht die Regelung in Artikeln 22, 23 und 24 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (ABl. Nr. L 281/31 vom 23.11.1995) einer nationalen Regelung entgegen, die neben den Eingriffsbefugnissen der Datenschutzbehörden und den Rechtsbehelfsmöglichkeiten des Betroffenen gemeinnützigen Verbänden zur Wahrung der Interessen der Verbraucher die Befugnis einräumt, im Falle von Verletzungen gegen den Verletzer vorzugehen?"

Der EuGH hat diesen Fall noch nicht entschieden, es gibt auch noch keine Stellungnahme des Generalanwalts. Art. 22 ff. DSRl und Art. 77 ff. DSGVO sind nicht identisch. Es ist aber wenig wahrscheinlich, dass der EuGH den Fall „Fashion ID" nach altem Recht entscheidet, ohne einen Fingerzeig zur Rechtslage nach der DSGVO zu geben.

Buchbesprechungen



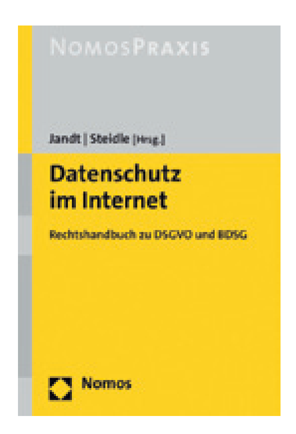
Ehmann, Eugen/Selmayr, Martin
DS-GVO Datenschutz-Grundverordnung – Kommentar
C. H. Beck, 2. Aufl. 2018, ISBN 978-3-406-72006 2, 1132 S., 149,00 €

(tw) Die Geschwindigkeit, mit welcher der C. H. Beck-Verlag mit einer zweiten Auflage der Kommentierungen zur DSGVO auf dem Markt ist, ist erstaunlich. Nach dem Paal/Pauly, dem Gola und dem Kühling/Buchner, die jeweils neu das BDSG und dessen Erläuterung aufgenommen haben, ist also jetzt der Ehmann/Selmayr aktualisiert. Mit Datenschutz lässt sich derzeit verlegerisch offenbar Geld verdienen. Die zweite Auflage von Ehmann/Selmayr baut vollständig auf der ersten Auflage auf (dazu DANA 2017, 179 f.), erweitert aber die Informationen um aktuelle Entwicklungen und neue Literatur und Gesetzgebung. Das deutsche BDSG sowie das österreichische DSG werden dokumentiert und teilweise knapp im Zusammenhang mit den Artikeln zur DSGVO erläutert. Neu ist z. B. auch bei Art. 95 eine Zusammenfassung der geplanten ePrivacy-Verordnung. Dies führte dazu, dass zwar die Seitenzahl in etwa gehalten wurde, doch das Format vergrößert werden musste.

Bei der Kommentierung der aktuellen Gesetzgebung wird die Umsetzung in Österreich teilweise kritisch und inhaltlich hinterfragt, wobei aber die kurz vor dem 25.05.2018 erfolgten Verschlechterungen nicht berücksichtigt wurden. Die begründete Kritik am deutschen BDSG fällt, wenn überhaupt, dagegen eher knapp und verhalten aus. Damit wird die Linie der ersten Auflage fortgeschrieben, die auch im Hinblick auf die EU-Gremien sich mit nötiger Kritik oder der Auseinandersetzung hierzu hinterm Berg hält. Dies ist dadurch erklärbar, dass viele der KommentatorInnen (zwei Frauen und 20 Männer) der Brüsseler

Datenschutz-Nomenklatura angehören.

Hierin liegt aber auch eine Stärke des Kommentars: die europäische Brille mit einem besonderen Auge auf den EuGH, die EU-Gremien und die Insider-Sicht. Dies macht das Werk auch für die wissenschaftliche Diskussion interessant, wobei Fragen der praktischen Umsetzung und der technische Datenschutz weniger ausführlich behandelt werden. Das Dilemma der Vielfalt der deutschen DSGVO-Literatur besteht weiterhin darin, dass sie nicht nur vielfältig, sondern auch selektiv ist, was es bei speziellen Einzelfragen immer nötig macht, mehrere Werke zu Rate zu ziehen, um vielleicht dann doch keine befriedigende Antwort zu bekommen. Dies gilt auch für den „Ehmann/Selmayr". Das liegt nicht nur daran, dass wir es hier mit einer neuen Rechtsmaterie zu tun haben.



Jandt, Silke/
Steidle, Roland, Datenschutz
Datenschutz im Internet
Rechtshandbuch zu DSGVO und BDSG
Nomos, 2018, 532 S., ISBN 978-3-8487-4856-3, 89,00 €

(tw) Das durch den Titel gegebene Versprechen, den Datenschutz im Internet umfassend in einer systematischen Darstellung präsentiert zu bekommen, macht neugierig. Das letzte Mal, dass ein Buch mit dem Titel „Datenschutz im Internet" veröffentlicht wurde, 2002 mit Peter Schaar als Autor, war zu einer technisch und rechtlich anderen Zeit. Die AutorInnen der einzelnen Kapitel steigern die Neugierde: MitarbeiterInnen von Aufsichtsbehörden (Ambrock, Jandt, Karg, Krasemann) WissenschaftlerInnen (Geminn, Hermonies, Selzer, Wilmer), ein Berater (Hammer) und Rechtsanwälte (Aßmus, Karsten, Steidle), zumeist jung, aus fortschrittlichen Publikationen schon bekannt und nicht durch allzu viele Publikationen festgelegt.

So schwingt die Hoffnung mit, dass „Datenschutz im Internet" gegen den Strich gebürstet wird. Die Lektüre lässt dann aber eine gewisse Ernüchterung eintreten: Das Buch zeichnet sich nicht durch disruptiven Datenschutz aus, sondern eher durch gediegene juristische Bearbeitung der Datenschutzthemen entlang der üblichen Argumentationslinien. Die Qualität resultiert aus einem hohen technischen Verständnis der Materie und einer gezielten Ausrichtung auf Internetanwendungen, wobei alle klassischen Datenschutzfragen in Bezug auf das Internet an Hand der jüngsten Veröffentlichungen (bis Mai 2018) bearbeitet werden: Webdienste, Cloud Computing, Office-Tools, Suchmaschinen, Webanalyse, Online-Werbung, Social Networks bis zu den sog. OTT-Kommunikationsdiensten. Anders als in den meisten juristischen Kommentierungen kommt der technisch-organisatorische Datenschutz dabei nicht zu kurz. Vielmehr wird, ausgehend von der Beschreibung der Technik eine qualifizierte rechtliche Bewertung vorgenommen. Angesichts der Vielzahl der AutorInnen finden sich Redundanzen und Behandlungen eines Themas aus verschiedenen Blickwinkeln, wobei aber – anders als bei vielen DSGVO/BDSG-Kommentaren – eine klare einheitliche Linie verfolgt wird.

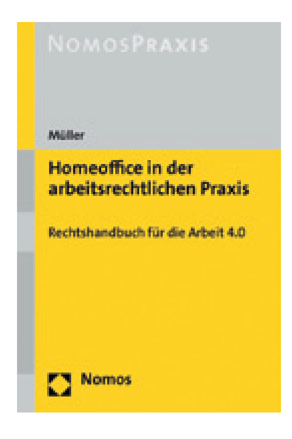
Hinsichtlich der Struktur orientiert sich die Darstellung an der der DSGVO und – was irritiert bzw. zumindest verblüfft – am EU-Kommissions-Entwurf zur E-Privacy-Verordnung. Das Handbuch wird so zu einer vorweggenommenen Kommentierung dieser E-Privacy-Verordnung. Dies ist zweifellos verdienstvoll, muss aber hinterfragt werden: Es ist eher unwahrscheinlich, dass eine Ratsposition zur E-Privacy-Verordnung im Jahr 2019 zustande kommt, und erst recht, dass der Trilog dazu abgeschlossen sein wird. Mit einem Wirksamwerden der Regeln ist also frühestens 2020/2021 zu rechnen. Für die Übergangszeit vertröstet das Handbuch auf die DSGVO und die E-Privacy-Richtlinie. Der Datenschutzteil des TMG wird einfach für überholt erklärt. So praktikabel diese Argumentation auch sein mag, so wenig kann sie dogmatisch und in den Einzelfallanwendungen überzeugen, werden doch damit geltende, parlamentarisch gefasste gesetzliche Regelungen per Kommentierung für obsolet erklärt.

Eine allzu leichtfertige Übernahme der Positionen des Handbuchs sollte deshalb nicht erfolgen, auch wenn, und das ist ein großer Pluspunkt, regelmäßig die Position der Aufsichtsbehörden nicht nur referiert, sondern qualifiziert vertreten wird. Insofern ist das Werk auch von hohem wissenschaftlichem Wert, wenngleich dann Gegenpositionen oft nur am Rande zu Wort kommen. So kann man – anders als die AutorInnen – wohl der Meinung sein, dass je nach Anwendungsfall das TMG weiterhin Bedeutung hat, dass Art. 5 Abs. 3 der E-Privacy-Richtlinie sich nur auf Cookies und nicht generell auf Tracking-Identifikatoren bezieht, oder mit dem deutschen Bundesgerichtshof, dass Anonymität bei inhaltlichen Internetveröffentlichungen durch die Meinungsfreiheit gefordert ist, auch bei Portalangeboten.

Das Thema Meinungsfreiheit im Netz spielt in der Praxis eine gewaltige Rolle und wird in dem Buch auch erwähnt, doch nur ganz am Rande, z. B. zu Bewertungsportalen oder zum Netzwerkdurchsetzungsgesetz. Auch der Konflikt zwischen Datenschutz und Urheber-, Patent-, Verlags- und Markenrechte wird nicht vertieft, obwohl genau dort aktuelle Streitlinien bestehen und in Zukunft liegen werden. Es wäre auch spannend gewesen, etwas über die kartell- bzw. wettbewerbsrechtliche und verbraucherrechtliche Seite der Internetdatenverarbeitung und deren Bezüge zum Datenschutz, zu den Monopol-Aktivitäten der großen US- oder auch der aufkommenden chinesischen Unternehmen und über das ökonomische und politische Profiling durch diese Firmen zu lesen. Das Privacy-Shield, eine zentrale Stütze der aktuellen Internet-Kommunikation, wird in gerade einmal 2 Randnummern eher neutral abgehandelt. Über die konkreten Praktiken von Facebook, Google, Microsoft, Apple und Amazon könnte man in einem Handbuch wie dem vorliegenden mehr erwarten.

Der Ansatz dieses Handbuchs, sich auf Internetdatenschutz zu konzentrieren,

ist bestechend. Sein Material und seine Positionen sind hoch relevant und hilfreich. In der Ausführlichkeit und klaren Positionsbestimmung ist es auf dem üppigen Markt der Veröffentlichungen zum Internetdatenschutz einzigartig. Es verschafft einen sehr guten juristischen Überblick und hat vorrangig den Datenschutz, nicht die Verarbeitungsinteressen im Blick. Für die praktische Lösung von schwierigen Problemlagen sollte aber auf weitere Quellen zurückgegriffen werden.



Müller, Stefan
Homeoffice in der arbeitsrechtlichen Praxis
Rechtshandbuch für die Arbeit 4.0
Nomos 2019, ISBN978-3-8487-4883-9, 260 S., 39,00 €

(tw) Das Arbeitsrecht und den Datenschutz zusammenzubringen ist ein schwieriges Unterfangen. Dieses Zusammenbringen wird zunehmend wichtig, zumal die Digitalisierung und Mobilisierung der Arbeit voranschreitet und dadurch das Kontroll- und Überwachungspotenzial bei der Arbeit steigt. Ein Werk zum „Homeoffice" und zur „Arbeit 4.0" ist daher für einen Datenschützer von großem Interesse.

Tatsächlich wird das „Rechtshandbuch" seinem Anspruch umfassend gerecht: Müller behandelt aus Sicht der Praxis fast sämtliche Rechtsfragen, die sich bei Aufnahme, Durchführung und Beendigung von Heimarbeit ergeben. Er geht dabei auf die Weisungsrechte der Arbeitgebers, die vielen dabei anzuwendenden gesetzlichen Regelungen vom Arbeitsschutz über das Arbeitszeitrecht, Fragen der Vergütung, der Kostentragung und Haftung bis hin zur kollektivvertraglichen Regulierung ein und beschreibt qualifiziert und unter Rückgriff auf weitere v. a. arbeitsrechtliche Literatur die komplexen Rechtsverhältnisse, die durch die Vermischung von privatem Wohnumfeld und Arbeitsleben entstehen. Erfreulich ist dabei die neutrale Darstellung, die den Eindruck vermeidet, dass der Autor sich auf eine Seite im Arbeitsverhältnis schlagen würde. Tatsächlich finden sich im gesamten Werk immer wieder Kästen, die praktische Ratschläge einmal für den Arbeitgeber, dann wieder für den Betriebsrat geben. Von praktischem Nutzen sind auch die im Anhang abgedruckten Checklisten. Formulierungsvorschläge, das Stichwortregister sowie das detaillierte Inhaltsverzeichnis, das einen zu Spezialfragen schnell fündig werden lässt.

Für Datenschützer besonders interessant sind seine Ausführungen zu den Kontroll- und Zutrittsrechten der Arbeitgebers, des Betriebsrats und anderer Betriebsangehöriger zur Wohnung des Arbeitnehmers als Arbeitsplatz. Dabei löst Müller die entstehenden Konfliktlagen – zumeist über Vereinbarungen – weitgehend interessengerecht. Interessant und vertretbar ist auch seine Ansicht, dass Aufsichtsbehörden zum Heimarbeitsplatz zwecks Kontrolle keinen Zugang haben, da dieser „Wohnung" und nicht „Geschäftsraum" ist.

Bei der Suche nach Antworten zu spezifischen Datenschutzfragen lässt einen der Autor dann aber oft allein oder weist in eine falsche Richtung: So erklärt er fälschlich den Art. 6 DS-GVO im Beschäftigungsverhältnis für anwendbar und ignoriert fast völlig die Regelung des § 26 BDSG. Zur hochkontroversen Frage der Kommunikationskontrolle äußert er sich überhaupt nicht. Die Aufsichtsbehörden „behördliche Datenschutzbeauftragte" zu nennen, ist befremdlich. Und dogmatisch unzutreffend wird es, wenn er z. B. die §§ 53 und 64 BDSG anwendet, die nur für den Justiz- und Polizeibereich anwendbar sind. Das schmälert aber die arbeitsrechtliche und weitgehend auch die datenschutzrechtliche Qualität der sonstigen Ausführungen nicht. Insofern ist das Werk gut auch für DatenschützerInnen geeignet, über den eigenen Tellerrand hinauszuschauen, wenn sie es mit Heimarbeit zu tun haben.



Arnold, Christian/Günther, Jens (Hrsg.)
Arbeitsrecht 4.0
Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt
C.H.Beck, München, 2018, 298 S., 59,00 €, ISBN 978-3-406-72213-4

(tw) Die Digitalisierung des Arbeitslebens hat nicht nur eine datenschutzrechtliche Seite, sondern hat Auswirkungen auf fast sämtliche Aspekte im Verhältnis zwischen Arbeitgebern und Beschäftigten: Produktions- und Arbeitsbedingungen, Formen des Beschäftigungsvertrags vom Abschluss bis zur Kündigung, Flexibilisierung mit der Folge der zeitlichen und örtlichen Entgrenzung, Qualifizierung, Direktionsrecht, Vergütungskonzepte, Arbeits- und Gesundheitsschutz, Haftung, Schutz des geistigen Eigentums und des Wettbewerbs, Mitbestimmungsrechte des Betriebsrats und natürlich auch Schutz des Rechts auf informationelle Selbstbestimmung der Beschäftigten.

Eine Stärke des Werkes ist dessen übergreifender Ansatz, der z. B. die verschiedenen modernen Beschäftigungsformen mit zumeist mehreren Beteiligten und die damit verbundenen Formen von Produktion und Vergütung sowie die sich daraus ergebenden sonstigen rechtlichen Konsequenzen – auch im Datenschutzrecht – im Detail erörtert: Digitale Arbeit erfolgt oft nicht mehr im klassischen eindimensionalen vertraglichen Abhängigkeitsverhältnis, sondern schließt Selbständigkeitsmodelle ebenso ein wie stufenweise, flexible Beschäftigungsbeziehungen, die steuer-, sozial-, zivil- wettbewerbs- sowie strafrechtlich und eben auch datenschutzrechtlich oft

nicht in klassische Muster einsortiert werden können. Bei der rechtlichen Bewertung wird auf die aktuelle Literatur und insbesondere höchstrichterliche Rechtsprechung, etwa des Bundesarbeitsgerichts, zurückgegriffen.

Zu den behandelten Rechtsthemen gibt es schon eine Menge Literatur. Das Handbuch von Arnold/Günther schafft es, diese vielen Themen knapp und zugleich differenziert, aussagekräftig und verständlich darzustellen. In den sieben Kapiteln präsentieren ohne große Redundanzen RechtsanwältInnen und HochschullehrerInnen die gesamte Bandbreite des digitalisierten Arbeitsrechts. Dabei wird nicht nur die rechtsdogmatische Seite beleuchtet, Erwähnung finden auch deren technische und historische Entwicklung sowie die politischen Erwägungen und Initiativen dazu. Eine eindeutige Parteinahme ist hierbei nicht zu erkennen, wohl aber schon, dass Adressat des Buches weniger Arbeitnehmervertretungen sind als RechtsanwältInnen, Personalabteilungen, Verbände und Arbeitgebervertretungen sowie – zumal es sich hier um noch nicht vollständig durchdrungene und um in der Entwicklung befindliche Sachverhalte handelt – WissenschaftlerInnen. Vereinzelte Praxishinweise bieten handwerkliche Hilfen. Die Ausführungen sind begleitet durch Verweise auf vertiefende Literatur.

Das Kapitel zum Datenschutz bleibt weitgehend hinter den spezifischen, erheblich umfangreicheren einschlägigen Darstellungen zurück. Doch werden hier aktuelle im Fluss befindliche Fragestellungen des Arbeitsrechts behandelt wie Bewerbungsportale, Videobewerbungen, Big Data und People Analytics, Smart Factory oder die Nutzung von Social Media und Verweise gegeben. Das neue Thema gemeinsamer Verantwortlichkeit wird noch nicht vertieft bearbeitet, wohl aber das gestufte Verhältnis zwischen DSGVO und BDSG. Dabei ist die Darstellung fast durchgängig korrekt und auf dem aktuellen Stand (Ausnahme S. 13, wo fälschlich der nur für Justiz/Inneres anwendbare § 71 BDSG zitiert wird). Damit erweist sich das Buch gerade für im Beschäftigtenbereich tätige DatenschützerInnen als äußerst hilfreich bei der Beantwortung von arbeitsrechtlichen Randfragen, die sich über den Umstand der Digitalisierung zum Rechtsverhältnis zwischen abhängig Beschäftigten und Beschäftigern stellen. Ein detailliertes Inhaltsverzeichnis, ein aussagekräftiges Stichwortverzeichnis sowie aktuelle Literaturhinweise erleichtern die Nutzung des Werks als Handbuch.

Cartoon



„Alexa, wann ist mein nächstes Meeting?“

„In Deiner Stimme sind Anzeichen einer Erkältung. Ich kann Dir ein Medikament empfehlen...“



Zu Risiken und Nebenwirkungen fragen Sie Ihren Datenschutzbeauftragten und Apotheker

https://www.sueddeutsche.de/digital/amazon-patent-alexa-soll-erkaelteten-nutzern-automatisch-medikamente-vorschlagen-1.4169311

Bild: AdobeStock